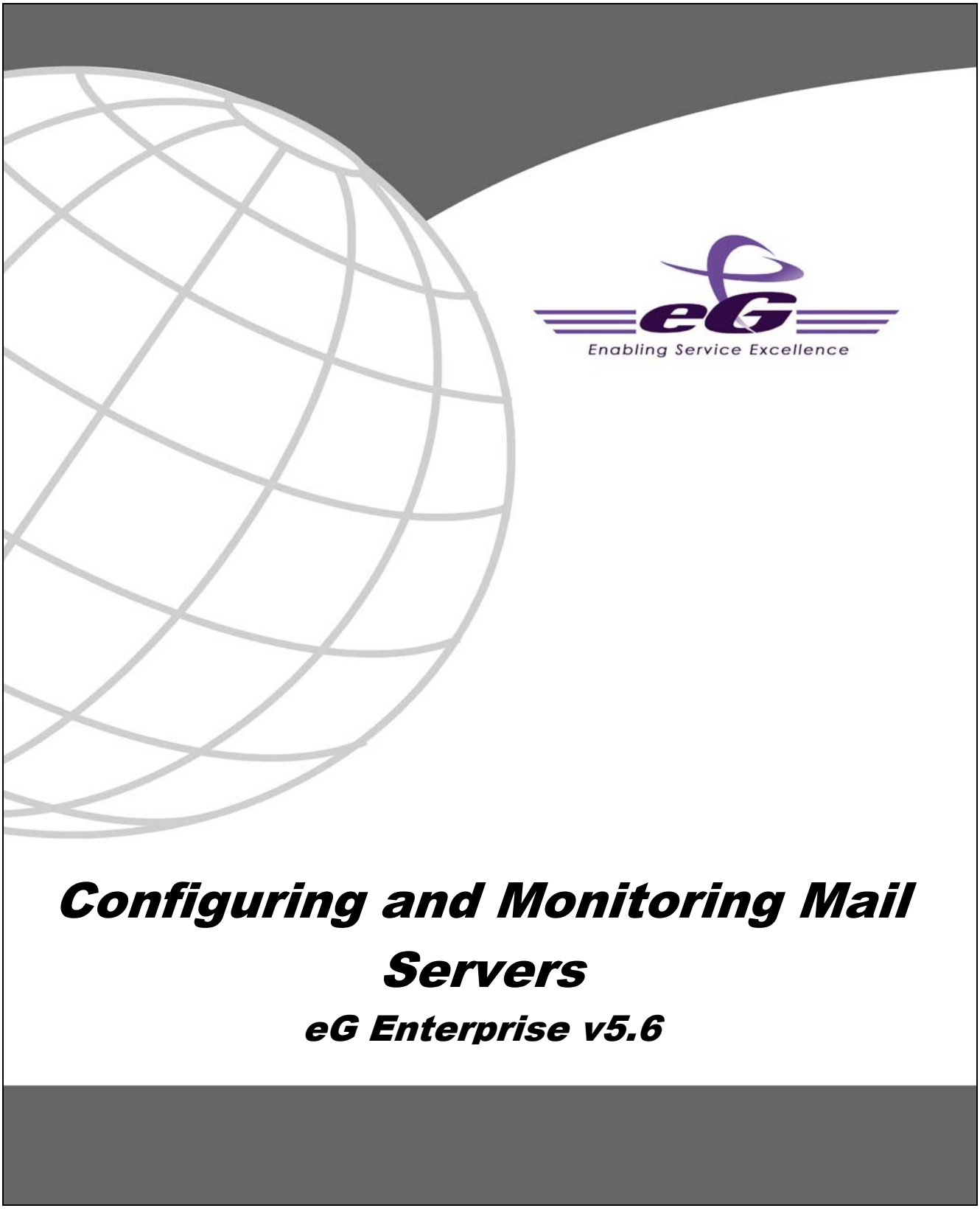

Configuring and Monitoring Mail Servers

eG Enterprise v5.6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations, Inc. eG Innovations, Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

© 2012 eG Innovations, Inc. All rights reserved.

Table of Contents

CONFIGURING AND MONITORING A LOTUS DOMINO MAIL SERVER 1

1.1 CONFIGURING A LOTUS DOMINO MAIL SERVER TO WORK WITH THE EG AGENT 1
1.1.1 Enabling SNMP for a Domino Server on Solaris 2
1.1.1.1 Installing and Configuring the Master SNMP Agent on the Domino Server 3
1.1.1.2 Configuring the Domino SNMP Agent 3
1.1.2 Enabling SNMP for a Domino Server on Linux 4
1.1.2.1 Installing and Configuring the Master SNMP Agent on the Domino Server 5
1.1.3 Configuring the Domino SNMP Agent 5
1.1.4 Enabling SNMP for a Domino Server on AIX 6
1.1.5 Enabling SNMP for Domino on Windows 7
1.1.5.1 Installing the SNMP Service 7
1.1.5.2 Installing the LNSNMP Agent on Windows 11
1.1.5.3 Configuring the LNSNMP Agent 12
1.2 CONFIGURING THE LOTUS DOMINO MAIL SERVER FOR THE DOMINONRPCTEST 13
1.3 ADMINISTERING THE EG MANAGER TO MONITOR THE LOTUS DOMINO MAIL SERVER 20
1.4 MONITORING THE LOTUS DOMINO MAIL SERVER 27

CONFIGURING AND MONITORING AN MS EXCHANGE SERVER 28

2.1 CONFIGURING AN MS EXCHANGE SERVER 5.5 TO WORK WITH THE EG MANAGER 28
2.2 ADMINISTERING THE EG MANAGER TO MONITOR AN MS EXCHANGE 5.5 SERVER 34
2.3 MONITORING THE MS EXCHANGE 5.5 SERVER 38

CONFIGURING AND MONITORING AN EXCHANGE 2000/2003 SERVER 39

3.1 CONFIGURING AN EXCHANGE SERVER 2000/2003 TO WORK WITH THE EG MANAGER 39
3.2 ADMINISTERING THE EG MANAGER TO MONITOR AN EXCHANGE 2000/2003 SERVER 44
3.3 MONITORING THE EXCHANGE 2000/2003 SERVER 53
3.4 TROUBLESHOOTING 53

CONFIGURING AND MONITORING A GENERIC MAIL SERVER 64

4.1 ADMINISTERING THE EG MANAGER TO MONITOR A GENERIC MAIL SERVER 64
4.2 MONITORING THE GENERIC MAIL SERVER 66

CONFIGURING AND MONITORING A QMAIL SERVER 67

5.1 CONFIGURING A QMAIL SERVER TO WORK WITH THE EG MANAGER 67
5.2 ADMINISTERING THE EG MANAGER TO MONITOR A QMAIL SERVER 67
5.3 MONITORING THE QMAIL SERVER 71

CONFIGURING AND MONITORING THE INSTANT MESSENGER OF THE EXCHANGE 2000 SERVER 72

6.1 ADMINISTERING THE EG MANAGER TO WORK WITH THE INSTANT MESSENGER 72
6.2 MONITORING THE INSTANT MESSENGER 73

CONFIGURING AND MONITORING EXTERNAL MAIL SERVERS 74

7.1 ADMINISTERING THE EG MANAGER TO WORK WITH AN EXTERNAL MAIL SERVER 74
7.2 MONITORING THE EXTERNAL MAIL SERVER 75

CONFIGURING AND MONITORING THE EXTERNAL EXCHANGE SERVER 76

8.1 ADMINISTERING THE EG MANAGER TO WORK WITH AN EXTERNAL EXCHANGE SERVER 76
8.2 MONITORING THE EXTERNAL MAIL SERVER 77

CONFIGURING AND MONITORING THE EXCHANGE CLUSTER SERVICE 78

9.1 ADMINISTERING THE EG MANAGER TO WORK WITH AN EXCHANGE CLUSTER SERVICE 78
9.2 MONITORING THE EXCHANGE CLUSTER SERVICE 80

CONFIGURING AND MONITORING THE IRONPORT ASYNCOS MAIL SERVER 81

10.1 ADMINISTERING THE EG MANAGER TO MONITOR AN IRONPORT ASYNCOS MAIL SERVER 81
10.2 MONITORING THE IRONPORT ASYNCOS MAIL SERVER 84

TROUBLESHOOTING 85

CONCLUSION 87

Table of Figures

Figure 1.1: Architecture of the Domino SNMP Agent 2
Figure 1.2: Selecting the Services tab 8
Figure 1.3: Selecting the SNMP service 8
Figure 1.4: Providing the path to the Windows NT files 9
Figure 1.5: The Add/Remove Programs option in the Control Panel window 9
Figure 1.6: Select the Add/Remove Windows Components option 10
Figure 1.7: Selecting the Management and Monitoring Tools option 10
Figure 1.8: Selecting the SNMP option 11
Figure 1.9: Providing the path to the Windows 2000 CD 11
Figure 1.10: Starting the Lotus Domino mail server 14
Figure 1.11: Opening the Administrator window 14
Figure 1.12: The Administration tab of the Administrator window 15
Figure 1.13: Selecting the Register option 15
Figure 1.14: Adding the details of the new user 16
Figure 1.15: Adding the user to the Registration queue 16
Figure 1.16: The new user appears in the list of current users 17
Figure 1.17: A screen displaying the details of the new user and a certificate 17
Figure 1.18: Detaching the certificate 18
Figure 1.19: Changing the certificate name 19
Figure 1.20: Managing a Domino Mail server 21
Figure 1.21: Viewing the tests to be configured for a Domino Mail server 21
Figure 1.22: Configuring the test parameters for a Domino Mail server 22
Figure 1.23: Configuring the Mailbox Size test 23
Figure 1.24: Selecting the tests to be enabled for Domino Mail server 25
Figure 1.25: Enabling the tests for the Domino Mail server 25
Figure 1.26: Selecting NRPC test from the unconfigured tests 26
Figure 1.27: Configuring the NRPC test 27
Figure 2.1： The Microsoft Exchange Administrator window 29
Figure 2.2: The Administrator window 30
Figure 2.3: Creating a mailbox for a user 30
Figure 2.4: Specifying the details of the new user account 31
Figure 2.5: The newly created mailbox being displayed in the Administrator window 32
Figure 2.6: The Services window displaying the eGurkhaAgent service 33
Figure 2.7: Configuring the eGurkhaAgent service to use the eG user name 34
Figure 2.8: Managing an Exchange 5.5 server 35
Figure 2.9: Selecting the tests to be enabled for Exchange 5.5 component type 36
Figure 2.10: Enabling the tests for the Exchange 5.5 component type 36
Figure 2.11: Selecting MsxMail test from the unconfigured tests 37
Figure 2.12: Configuring the MsXMail test 38
Figure 3.1: Opening the Microsoft Exchange Active Directory Users and Computers window 40
Figure 3.2: Creating a new Exchange mail box for user *john* 40
Figure 3.3: Specifying the details of the new user account 41
Figure 3.4: Specifying the password 41
Figure 3.5: Creating a mailbox 42
Figure 3.6: Summary of the specifications 42
Figure 3.7: The E-mail Addresses tab 43
Figure 3.8: Selecting Microsoft Mail Address as the address type 44
Figure 3.9: Specifying the properties of the address type 44
Figure 3.10: Viewing the list of unmanaged Exchange 2000/2003 servers 45
Figure 3.12: The list of unconfigured tests for an Exchange 2000/2003 server 46
Figure 3.13: Mail test for an Exchange 2000/2003 server 47
Figure 3.14: Configuring the Disconnected Mailboxes test 47
Figure 3.15: Selecting the tests to be enabled for Exchange 2000/2003 server 49
Figure 3.16: Enabling the tests for the Exchange 2000/2003 server 49
Figure 3.17:Selecting Mapi Mail Service test from the unconfigured tests 50
Figure 3.18: The Active Directory Users and Computers console 51
Figure 3.19: Properties of the chosen user account 51
Figure 3.20: Configuring the XchgMailBox test 53
Figure 3.21: Message box indicating a problem in sending mails 54
Figure 3.22: Selecting the 'Add/Remove Features' option 55
Figure 3.23: Choosing to customize the Outlook installation 55
Figure 3.24: Viewing the currently installed applications 56
Figure 3.25: Selecting the Collaboration Data Objects option 56
Figure 3.26: The End-use license agreement 57
Figure 3.27: Selecting the install directory 57

Figure 3.28: Installing Orktools.exe 58
Figure 3.29: Accepting the license agreement for admpack.exe 58
Figure 3.30: Specifying the location of the admpack files 59
Figure 3.31: Completion of admpack installation 59
Figure 3.32: Opening the System Manager of the Microsoft Exchange Server 2000 59
Figure 3.33: Creating a new Public Folder 60
Figure 3.34: Naming the new public folder 60
Figure 3.35: Opening the OutlookSecurity.oft template file 61
Figure 3.36: Selecting the Outlook Security Settings folder 61
Figure 3.37: Publishing the form 62
Figure 3.38: Specifying a name for the form 62
Figure 3.39: Choosing the Outlook Security Form option 63
Figure 3.40: Selecting the Reviewer role 63
Figure 4.1: Selecting the type of component to be added 65
Figure 4.2: Adding the details of a new mail server 65
Figure 4.3: A page displaying a summary of the new mail server details 66
Figure 4.4: A page displaying the tests the need to be configured for the Generic mail server 66
Figure 5.1: Selecting the Qmail server to be monitored 68
Figure 5.2: Managing the selected Qmail server 69
Figure 5.3: A page displaying the tests the need to be configured for the Qmail server 69
Figure 5.4: Configuring the Qmail Delivery test 69
Figure 5.5: Configuring the Qmail Queues test 70
Figure 6.1: Adding the Instant Messenger 72
Figure 7.1: Adding an External mail server 74
Figure 7.2: A page listing the unconfigured tests for the External mail server 75
Figure 8.1: Adding an External Exchange server 76
Figure 8.2: A page listing the unconfigured tests for the External mail server 77
Figure 9.1: Adding an Exchange cluster service 78
Figure 9.2: A segment containing the cluster service and the Exchange servers 79
Figure 9.3: A page listing the unconfigured tests for the Extchange cluster service and the individual Exchange servers in the cluster 79
Figure 10.1: Selecting the type of component to be added 81
Figure 10.2: Adding the details of a new IronPort AsyncOS Mail Server 82
Figure 10.3: A page displaying a summary of the new IronPort AsyncOS Mail Server details 82
Figure 10.4: A page displaying the tests that need to be configured for the IronPort AsyncOS Mail Server 82
Figure 10.5:Configuring the Asyncos Fan Status test 83

Chapter 1

Configuring and Monitoring a Lotus Domino Mail Server

This chapter enables you to gain a clear understanding of the procedures that go into:

- Configuring a Lotus Domino Server to work with an eG agent
- Administering the eG manager to monitor the Lotus Domino mail server
- Monitoring the Lotus Domino mail server

1.1 Configuring a Lotus Domino Mail Server to work with the eG Agent

eG Enterprise has developed an exclusive monitoring model for the Domino mail server, which employs an eG agent to continuously monitor the performance of the server. This eG agent executes tests on the server, which contact the Domino SNMP agent for performance information.

Domino SNMP Agent services are provided by two types of programs:

- LNSNMP -- The Lotus Notes SNMP agent. As an independent application, LNSNMP is insulated from most Domino server malfunctions and, by itself, adds negligible overhead to the server.
- Two Domino server add-ins -- the QuerySet Handler and the Event Interceptor.
    - The QuerySet Handler and the Event Interceptor depend on the Domino server; if the server fails for any reason, these programs fail as well.

The following components comprise the Domino SNMP Agent architecture:

- A platform-specific **Master SNMP Agent** -- An independent, non-Lotus, agent usually supplied with the operating system platform that provides SNMP services for the machine. This SNMP Agent transports the SNMP traps and Get/Set responses across the network to the management station.
- The **Domino SNMP Agent** consisting of:

- *LNSNMP Agent* -- The Lotus Notes SNMP agent, which receives trap notifications from the Event Interceptor and then forwards them to the management station using the platform-specific SNMP Agent. LNSNMP also handles requests for Domino-related information from the management station by passing the request to the QuerySet Handler and responding back to the management station.
- *QuerySet Handler* -- Which queries server statistics information, sets the value of configurable Domino-based parameters, and returns Domino statistics information to LNSNMP, which then forwards the information to the management station using the platform-specific master SNMP Agent.
- *Event Interceptor* -- Which responds to the SNMP Trap notification for Domino Event Handlers by instructing LNSNMP to issue a trap.

- The **Domino MIB** -- A standard Management Information Base (MIB) file for Lotus Domino servers that can be compiled and used by a network management program such as eG Enterprise.

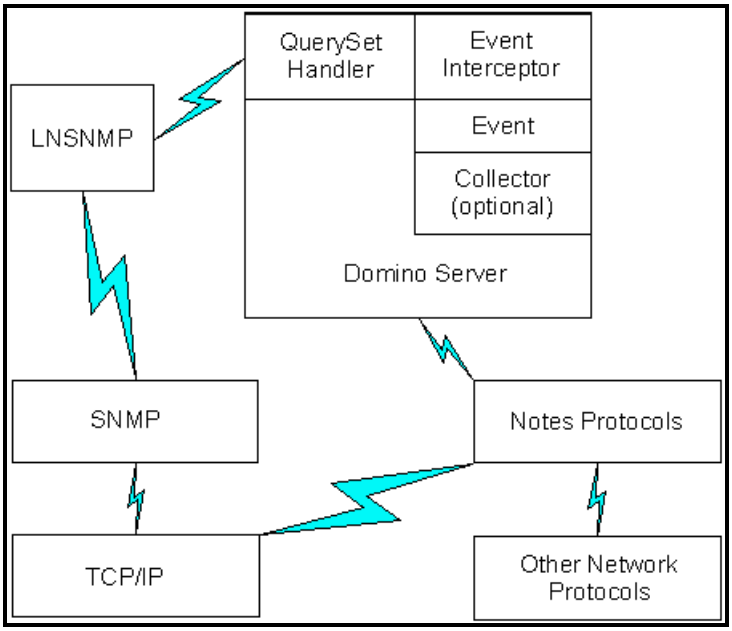

Figure 1.1: Architecture of the Domino SNMP Agent

1.1.1 Enabling SNMP for a Domino Server on Solaris

To enable SNMP on a Domino server on Solaris, follow the broad steps given below:

- Install the Master SNMP agent on the Domino server
- Configure the Domino SNMP agent to communicate with the Master SNMP agent
- Each of these steps has been discussed in great detail below.

1.1.1.1 Installing and Configuring the Master SNMP Agent on the Domino Server

On Solaris platform, the Domino SNMP Agent uses the SMUX protocol, per RFC 1227, to communicate with the system's Master SNMP Agent. The Solaris Master SNMP Agent does not support the SMUX protocol, making it necessary to substitute a Master SNMP Agent that does. On Solaris platforms, Domino includes a suitable NET-SNMP Master Agent, called NET-SNMPD, already configured to support the SMUX protocol and the Domino SNMP Agent.

Note:

Before using NET-SNMPD, disable any existing Master SNMP Agent. Please follow the steps below for disabling an existing Master SNMP Agent running on Solaris.

- Log in as root.
- Stop the **snmpdx** daemon by typing, **/etc/rc3.d/S76snmpdx stop**.
- Disable the **snmpdx** daemon by issuing the command, **mv /etc/rc3.d/S76snmpdx /etc/rc3.d/s76snmpdx**.

To use the NET-SNMPD that is provided with Domino, do the following:

1. Login as the root user.
2. Next, install the NET-SNMPD files. Enter this command, changing the Domino executable path if necessary: **cp /opt/lotus/notes/latest/sunspa/net-snmpd* /etc**
3. Arrange for NET-SNMPD to be restarted after a reboot. Enter these commands:

   ln -f -s /etc/net-snmpd.sh /etc/init.d/net-snmpd

   ln -f -s /etc/init.d/net-snmpd /etc/rc2.d/S76net-snmpd

   ln -f -s /etc/init.d/net-snmpd /etc/rc1.d/K76net-snmpd
4. After installation, proceed to configure and start NET-SNMPD. Here is how:
5. Udate the **/etc/net-snmpd.conf** file with appropriate community names for your remote management infrastructure. Community names are set using the **rocommunity** and **rwcommunity** directives. For instance, to set a community named **nppublic**, the command would be: **Set rocommunity value to nppublic**
6. To manually start NET-SNMPD, login as the root user and issue the command, **/etc/net-snmpd.sh start**. To stop NET-SNMPD, use this command: **/etc/net-snmpd.sh stop**

1.1.1.2 Configuring the Domino SNMP Agent

The Domino SNMP Agent configuration on Solaris involves the following:

- Configuring the LNSNMP agent to work with the Master SNMP Agent that is provided with Domino
- Completing the configuration by starting the add-in tasks

Before attempting to configure the Domino SNMP agent, ensure the following:

- The Solaris Master SNMP Agent provided with Domino should be properly installed and configured on the server. Refer to the steps discussed in Section 1.1.1.1 for the procedure.
- TCP/IP and SNMP should be properly installed and configured on the server. Ensure that the Domino executable and the Domino data directories are in your search path.
- The Domino SNMP Agent is set up to run automatically. Once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino, stop the LNSNMP process, before beginning the upgrade process.

To configure the LNSNMP agent, do the following:

1. Login as the root-user.
2. Stop the LNSNMP process. Enter this command: **lnsnmp.sh stop**
3. Stop the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh stop**
4. Start the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh start**
5. Start the LNSNMP process using the command, **lnsnmp.sh start**
6. Create a link to the LNSNMP script. Enter this command, changing the Domino executable path if necessary: **ln -f -s /opt/lotus/notes/latest/sunspa/lnsnmp.sh /etc/init.d/lnsnmp**
7. Arrange for LNSNMP to be restarted after a reboot. Enter these commands:

   ln -f -s /etc/init.d/lnsnmp /etc/rc2.d/S77lnsnmp

   ln -f -s /etc/init.d/lnsnmp /etc/rc1.d/K77lnsnmp

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks. To achieve this, do the following:

1. To support SNMP queries, start the QuerySet add-in task. Enter this command on the Domino Server console: **load queryset**
2. To support SNMP traps for Domino events, start the Event Interceptor add-in task. Enter this command on the Domino Server console: **load intrcpt**
3. To support Domino statistic threshold traps, start the Statistic Collector add-in task. Enter this command on the Domino Server console: **load collect**
4. Arrange for the add-in tasks to be restarted automatically when Domino is next restarted. Add **queryset** and/or **intrcpt** and **collect** to the ServerTasks variable in Domino's **notes.ini** file.

   *ServerTasks =Update,Replica,Router,Amgr,AdminP,CalConn,Sched,LDAP,**queryset,intrcpt,collect***

1.1.2 Enabling SNMP for a Domino Server on Linux

To enable SNMP on a Domino server on Linux, follow the broad steps given below:

- Install the Master SNMP agent on the Domino server

- Configure the Domino SNMP agent to communicate with the Master SNMP agent
- Each of these steps has been discussed in great detail below.

1.1.2.1 Installing and Configuring the Master SNMP Agent on the Domino Server

Like the Solaris platform, on Linux also the Domino SNMP Agent uses the SMUX protocol, per RFC 1227, to communicate with the system's Master SNMP Agent. Some Linux distributions include a Master SNMP Agent that supports the SMUX protocol; others do not. On Linux platforms, Domino includes a suitable NET-SNMP Master Agent, called NET-SNMPD, already configured to support the SMUX protocol and the Domino SNMP Agent.

Note:

Before using NET-SNMPD, disable any existing MasterSNMP Agent. For information on disabling an existing Master SNMP Agent, see your Master SNMP Agent's documentation.

To use the NET-SNMPD that is provided with Domino, do the following:

1. Login as the root user.
2. Next, install the NET-SNMPD files. Enter this command, changing the Domino executable path if necessary: **cp /opt/lotus/notes/latest/linux/net-snmpd* /etc**
3. Arrange for NET-SNMPD to be restarted after a reboot. Enter these commands:

   ln -f -s /etc/net-snmpd.sh /etc/rc.d/init.d/net-snmpd

   chkconfig --add net-snmpd

   chkconfig net-snmpd on
4. After installation, proceed to configure and start NET-SNMPD. Here is how:
5. Udate the **/etc/net-snmpd.conf** file with appropriate community names for your remote management infrastructure. Community names are set using the **rocommunity** and **rwcommunity** directives. For instance, to set a community named **nppublic**, the command would be, **Set rocommunity value to nppublic**.
6. To manually start NET-SNMPD, login as the root user and issue the command, **/etc/net-snmpd.sh start**. To stop NET-SNMPD, use the command, **/etc/net-snmpd.sh stop**.

1.1.3 Configuring the Domino SNMP Agent

The Domino SNMP Agent configuration on Linux involves the following:

- Configuring the LNSNMP agent to work with the Master SNMP Agent that is provided with Domino on Linux
- Completing the configuration by starting the add-in tasks

Before attempting to configure the Domino SNMP agent, ensure the following:

- The Linux Master SNMP Agent provided with Domino should be properly installed

and configured on the server. Refer to the steps discussed in Section 1.1.2.1 for the procedure.

- TCP/IP and SNMP should be properly installed and configured on the server. Ensure that the Domino executable and the Domino data directories are in your search path.
- The Domino SNMP Agent is set up to run automatically. Once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino, stop the LNSNMP process, before beginning the upgrade process.

To configure the LNSNMP agent, do the following:

1. Login as the root-user.
2. Stop the LNSNMP process. Enter this command: **lnsnmp.sh stop**
3. Stop the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh stop**
4. Start the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh start**
5. Start the LNSNMP process using the command, **lnsnmp.sh start**.
6. Arrange for LNSNMP to be restarted after a reboot. Enter these commands:

   ln -f -s /opt/lotus/notes/latest/linux/lnsnmp.sh /etc/rc.d/init.d/lnsnmp

   chkconfig --add lnsnmp

   chkconfig lnsnmp on

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks. To achieve this, do the following:

1. To support SNMP queries, start the QuerySet add-in task. Enter this command on the Domino Server console: **load quryset**
2. To support SNMP traps for Domino events, start the Event Interceptor add-in task. Enter this command on the Domino Server console: **load intrcpt**
3. To support Domino statistic threshold traps, start the Statistic Collector add-in task. Enter this command on the Domino Server console: **load collect**
4. Arrange for the add-in tasks to be restarted automatically when Domino is next restarted. Add **quryset** and/or **intrcpt** and **collect** to the ServerTasks variable in Domino's **notes.ini** file.

   *ServerTasks =Update,Replica,Router,Amgr,AdminP,CalConn,Sched,LDAP,**quryset,intrcpt,collect***

1.1.4 Enabling SNMP for a Domino Server on AIX

To enable SNMP on an AIX Domino server, you will have to configure the Domino SNMP agent (i.e., the LNSNMP process) to communicate with the SNMPD subsystem (on AIX) using the SMUX protocol.

However, prior to configuring the Domino SNMP agent, make sure that the following are in place:

- TCP/IP and SNMP should be properly installed and configured on the server. Also, make sure that the Domino executable and the Domino data directories are in your search path

- The trap destinations and **community names for AIX should be appropriately configured in the /**etc/snmpd.conf file for your remote management infrastructure. Remember to keep the view identifiers unique for each trap destination.
- The Domino SNMP Agent is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino you should stop the LNSNMP process before beginning the upgrade process.

Next, proceed to configure the Domino SNMP agent, using the procedure explained below:

1. Login as the root user.
2. Stop the LNSNMP process. Enter this command: **lnsnmp.sh stop**
3. Stop the SNMPD (SNMP Daemon) subsystem. The Simple Network Management Protocol (SNMP) daemon is a background server process that can be run on any Transmission Control Protocol/Internet Protocol (TCP/IP) workstation host. The daemon, acting as SNMP agent, receives, authenticates, and processes SNMP requests from manager applications. This daemon is installed and started by default on AIX systems. To stop SNMPD, enter this command: **stopsrc -s snmpd**
4. Configure SNMPD to accept LNSNMP as an SMUX peer. Add the following line to the **/etc/snmpd.peers** file: **"Lotus Notes Agent" 1.3.6.1.4.1.334.72 "NotesPasswd"**
5. Configure SNMPD to accept an SMUX association from LNSNMP. Add the following line to **/etc/snmpd.conf: smux 1.3.6.1.4.1.334.72 NotesPasswd**
6. Start the SNMPD subsystem. Enter this command: **startsrc -s snmpd**
7. Start the LNSNMP process. Enter this command: **lnsnmp.sh start**
8. Create a link to the LNSNMP script. Enter this command, changing the Domino executable path if necessary: **ln -f -s /opt/lotus/notes/latest/ibmpow/lnsnmp.sh /etc/lnsnmp.rc**
9. Arrange for LNSNMP to be restarted after a reboot. Add the following line to the end of the **/etc/rc.tcpip** file: **/etc/lnsnmp.rc start**

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks, using the procedure discussed in Section 1.1.3.

1.1.5 Enabling SNMP for Domino on Windows

To enable SNMP on a Windows Domino server, follow the broad steps given below:

Install the Windows SNMP service on the target host

Install the LNSNMP agent (i.e., the Lotus Domino SNMP agent) on the target host

Configure the Lotus Domino SNMP agent as a service on the target host

Each of these steps is discussed in great detail in the sections to come.

1.1.5.1 Installing the SNMP Service

To install the SNMP service on Windows NT, do the following:

1. Login to the Windows NT system as an administrator.

2. Right-click on the **Network Neighbourhood** icon on the desktop, and select the **Properties** option from the shortcut menu.

3. Next, select the **Services** tab in the dialog box that appears, and click on the **Add** button within (see Figure 1.2).

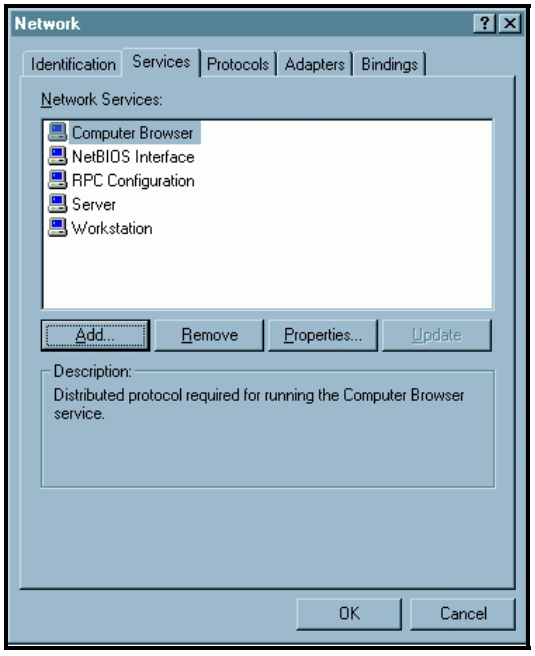

Figure 1.2: Selecting the Services tab

4. From the list of services that appears, choose the **SNMP Service** (see Figure 1.3).

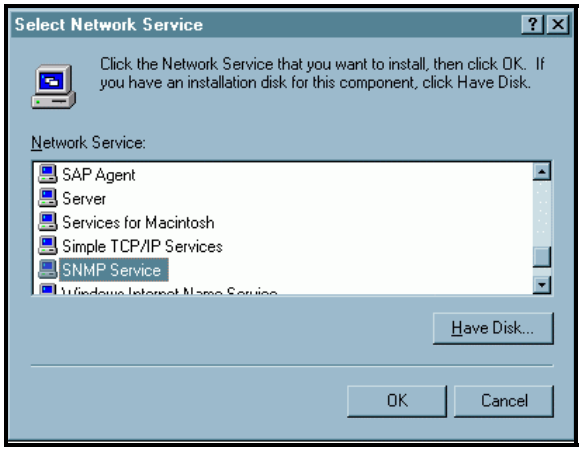
Select Network Service
Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.
Network Service:
SAP Agent
Server
Services for Macintosh
Simple TCP/IP Services
SNMP Service
Have Disk...
OK
Cancel

Figure 1.3: Selecting the SNMP service

5. If you are then prompted for the path to the Windows NT files, provide the correct path, and click on the **Continue** button to begin installing the **SNMP Service** (see Figure 1.4).

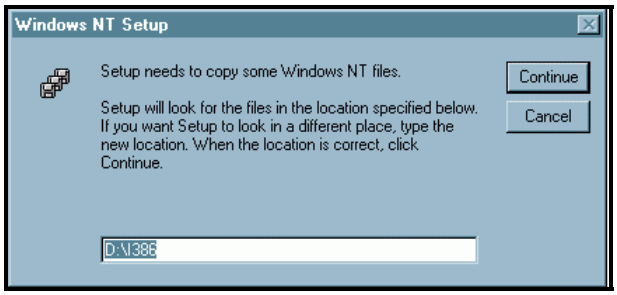
Windows NT Setup
Setup needs to copy some Windows NT files.
Setup will look for the files in the location specified below. If you want Setup to look in a different place, type the new location. When the location is correct, click Continue.
Continue
Cancel
D:\I386

Figure 1.4: Providing the path to the Windows NT files

6. Once installation is complete, reboot the system.
7. After the system reboots, ensure that **all service packs are re-installed**.

To install the SNMP service on Windows 2000, do the following:

1. Login to the Windows 2000 system as an administrator.
2. Click on the **Start** button on the taskbar, and follow the menu sequence: Settings -> Control Panel.
3. Double-click on the **Add/Remove Programs** option in the Control Panel window (see Figure 1.5).

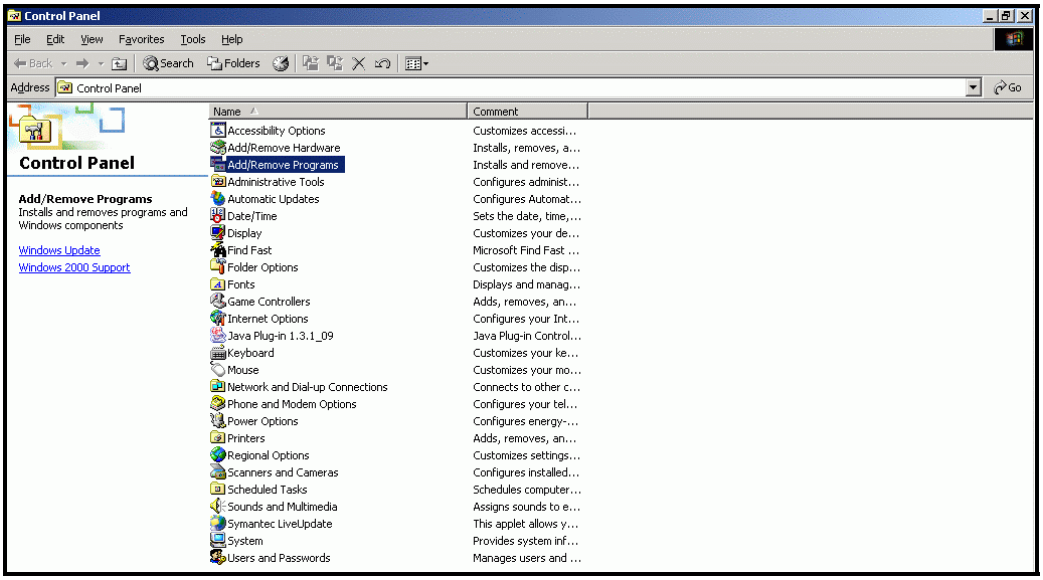

Figure 1.5: The Add/Remove Programs option in the Control Panel window

4. Next, select the **Add/Remove Windows Components** option from the **Add/Remove Programs** dialog box (see Figure 1.6).

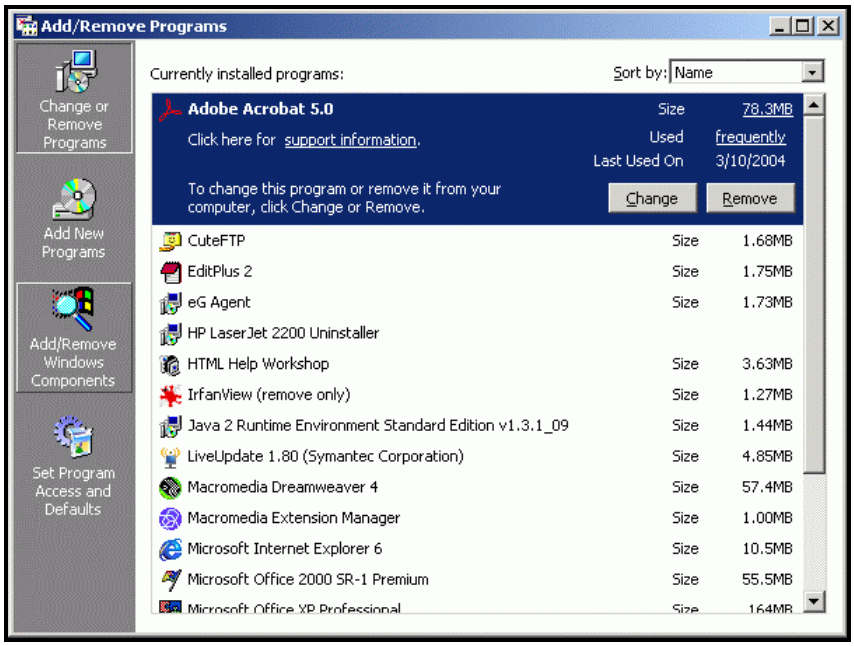
Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Currently installed programs:
Sort by: Name
Adobe Acrobat 5.0
Size 78.3MB
Click here for support information.
Used frequently
Last Used On 3/10/2004
To change this program or remove it from your computer, click Change or Remove.
Change
Remove
CuteFTP Size 1.68MB
EditPlus 2 Size 1.75MB
eG Agent Size 1.73MB
HP LaserJet 2200 Uninstaller
HTML Help Workshop Size 3.63MB
IrfanView (remove only) Size 1.27MB
Java 2 Runtime Environment Standard Edition v1.3.1_09 Size 1.44MB
LiveUpdate 1.80 (Symantec Corporation) Size 4.85MB
Macromedia Dreamweaver 4 Size 57.4MB
Macromedia Extension Manager Size 1.00MB
Microsoft Internet Explorer 6 Size 10.5MB
Microsoft Office 2000 SR-1 Premium Size 55.5MB
Microsoft Office XP Professional Size 164MB

Figure 1.6: Select the Add/Remove Windows Components option

5. Then, a list of windows components that can be added will appear. Select the **Management and Monitoring Tools** option from this list, and click the **Details** button to view more details about it (see Figure 1.7).

Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Indexing Service 0.0 MB
Internet Explorer 0.0 MB
Internet Information Services (IIS) 18.2 MB
Management and Monitoring Tools 0.9 MB
Message Queuing Services 2.6 MB
Description: Includes tools for monitoring and improving network performance.
Total disk space required: 0.2 MB
Space available on disk: 2283.8 MB
Details...
< Back
Next >
Cancel

Figure 1.7: Selecting the Management and Monitoring Tools option

6. From the list that appears next, select the **Simple Network Management Protocol** (SNMP) option to add it. Then, click the **OK** button (see Figure 1.8).

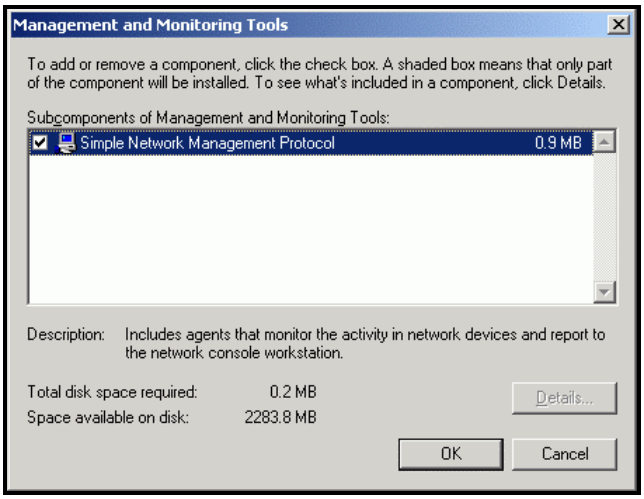
Management and Monitoring Tools
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Management and Monitoring Tools:
Simple Network Management Protocol 0.9 MB
Description: Includes agents that monitor the activity in network devices and report to the network console workstation.
Total disk space required: 0.2 MB
Space available on disk: 2283.8 MB
Details...
OK
Cancel

Figure 1.8: Selecting the SNMP option

7. You will then return to Figure 1.7. Click the **Next** button here to proceed with installing the **SNMP** service.
8. If you are prompted for the path to the Windows 2000 installation CD, provide the correct path, and click on the **OK** button to begin installing the **SNMP** service (see Figure 1.9).

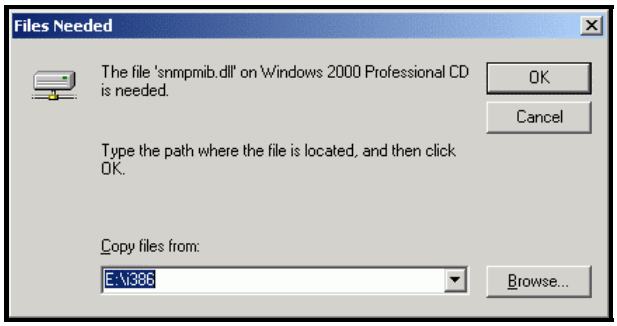

Figure 1.9: Providing the path to the Windows 2000 CD

1.1.5.2 Installing the LNSNMP Agent on Windows

To install the LNSNMP agent (version 5.0), do the following:

1. Run the **nvinst.exe** executable that is available in the **<DOMINO_INSTALL_DIR>/w32intel** folder.
2. Once execution begins, setup will prompt you to choose one of the following options:

```
Domino Management Agent for Windows NT installation.
Copyright (c) 1994-1999, Lotus Development Corporation.  All Rights
Reserved.

Lotus Domino Management Agent Install (Version 5.0)
Installation Options
-------------------------------------------------
```

```
1) Install Domino SNMP Agent Software
2) Install Domino Mail Reflector Software
3) Install Both Options 1 and 2
Q) Quit Installation

Choice (1/2/3/Q): 1
```

3. To install the LNSNMP agent, enter **1** as the **Choice**.
4. Setup will then request your confirmation for adding the Collector task. Enter **y** to add the task.

```
The "Collector" task is not currently configured to run on this system.
This task is necessary if you want Notes to generate events based on
statistics thresholds.

Do you want to add this task now? (y/n): y
```

5. Once the LNSNMP agent installation completes, the following message will appear:

```
Domino Management Agent successfully installed.
Please reboot the system for the changes to take effect.

D:\Lotus\Domino\w32intel>

After Rebooting start the LNSNMP Service first
And then start the Domino Server.
```

1.1.5.3 Configuring the LNSNMP Agent

Prior to configuring the LNSNMP agent, ensure the following:

- Before using the Domino SNMP Agent, make sure TCP/IP and SNMP are properly installed and configured on the server. Also, make sure that the Domino executable and the Domino data directories are in your search path.
- If you need to add the Windows SNMP Service to your system, be prepared to reinstall any Windows service packs immediately after adding the Windows SNMP Service.
- The Windows SNMP Service is configured by double-clicking the Network icon in the Control Panel, then selecting the Services tab, then selecting SNMP Service, and then clicking the Properties button. You will want to configure appropriate trap destinations and community names for your remote management infrastructure.
- The Domino SNMP Agent is configured as a Windows Service and is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino

you should stop the LNSNMP and Windows SNMP Services before beginning the upgrade process.

To configure the LNSNMP agent, do the following:

1. Stop the LNSNMP and SNMP services using the following commands:

   net stop lnsnmp

   net stop snmp

2. Configure the Lotus Domino SNMP agent as a service using the following command:

   lnsnmp –Sc

3. Start the SNMP and LNSNMP services by issuing the following commands:

   net start snmp

   net start lnsnmp

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks, using the procedure discussed in Section Configuring the Domino SNMP Agent.

Note:

If you ever need to undo the configuration of the Lotus Domino SNMP Agent as a service, enter this command: **lnsnmp -Sd**

1.2 Configuring the Lotus Domino Mail Server for the DominoNrpcTest

The DominoNrpcTest executed by an eG external agent simulates clients sending and receiving mails via a Lotus Domino mail server, using the NRPC protocol. This test monitors the availability and performance of the Lotus Domino mail server. The two main parameters of this test are:

- The user name of a mailbox on the Domino server that the test uses to send and receive mails
- The password for the user mailbox

The following are the pre-requisites for the functioning of this test:

1. The eG external agent that is executing the DominoNrpcTest, should be installed on a Windows NT/2000 server/client in the same domain as the Lotus Domino mail server.
2. While deciding on a mailbox to be used for configuring the test, the administrator should first check whether the mailbox exists on the Domino server. If no mailboxes exist, then create one using the instructions given below and then configure the same for the test:
   - Start the LNSNMP service by specifying the following command at the

command prompt: **net start LNSNMP**

- Then, start the mail server using the following menu sequence (see Figure 1.10):

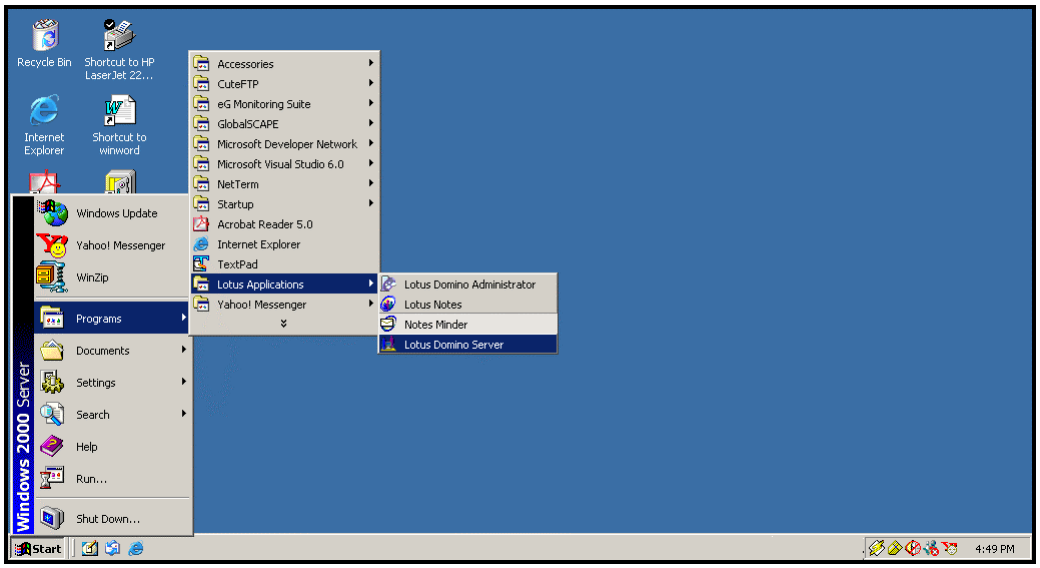

Figure 1.10: Starting the Lotus Domino mail server

- Once the server starts successfully, open the Lotus Domino Administrator window using the following menu sequence (see Figure 1.11):

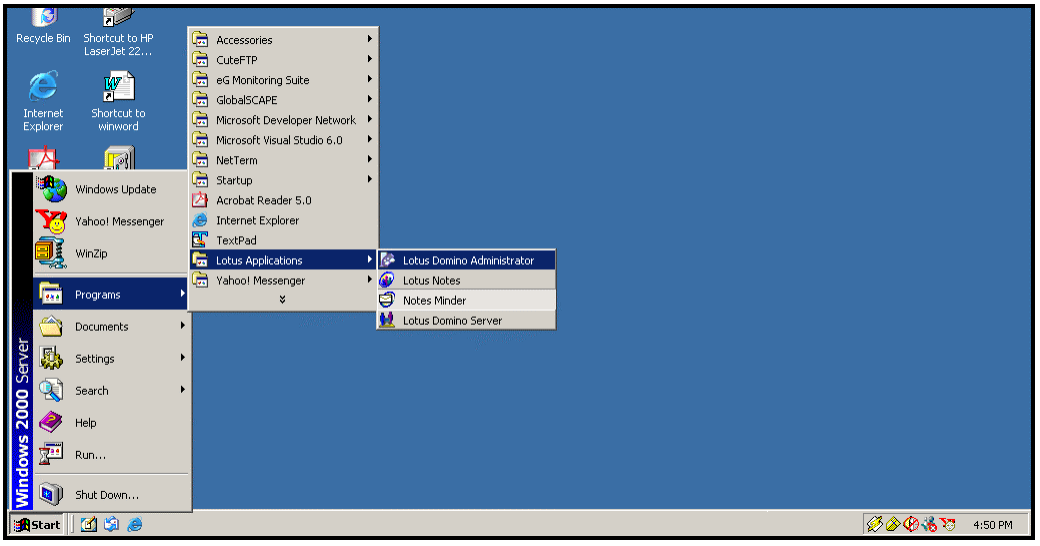

Figure 1.11: Opening the Administrator window

- From the Administrator window that appears, select the **Administration** tab (see Figure 1.12). The **People & Groups** tab appears by default (see Figure 1.12).

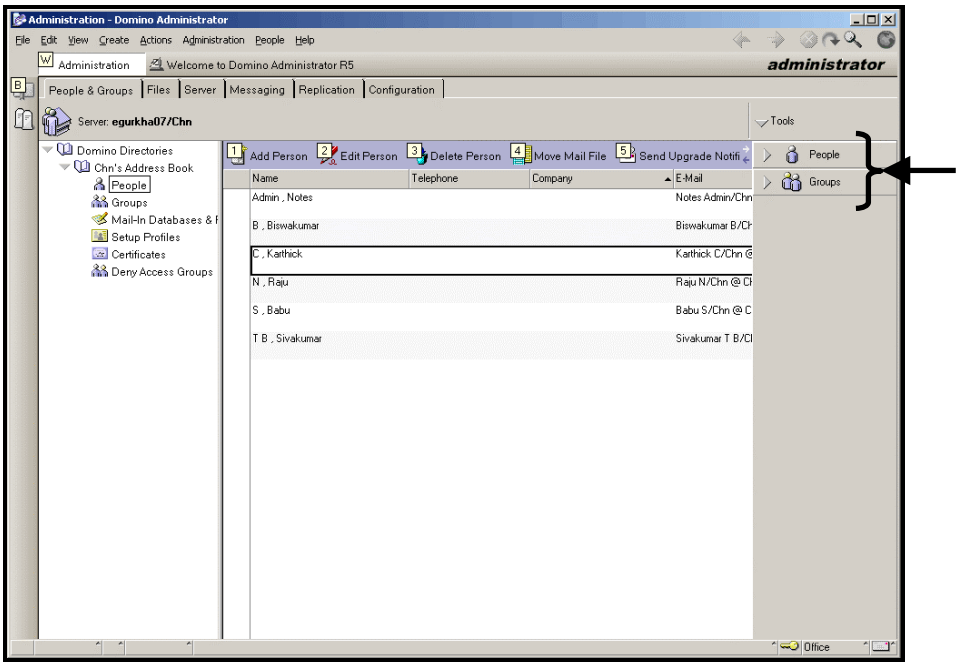

Figure 1.12: The Administration tab of the Administrator window

- Figure 1.12 also displays two options - **People** and **Groups** – on the right side of the window. Clicking on the **People** option reveals a whole list of menu options (see Figure 1.13). Select the **Register** option from the drop-down menu (see Figure 1.13) to create a new user.

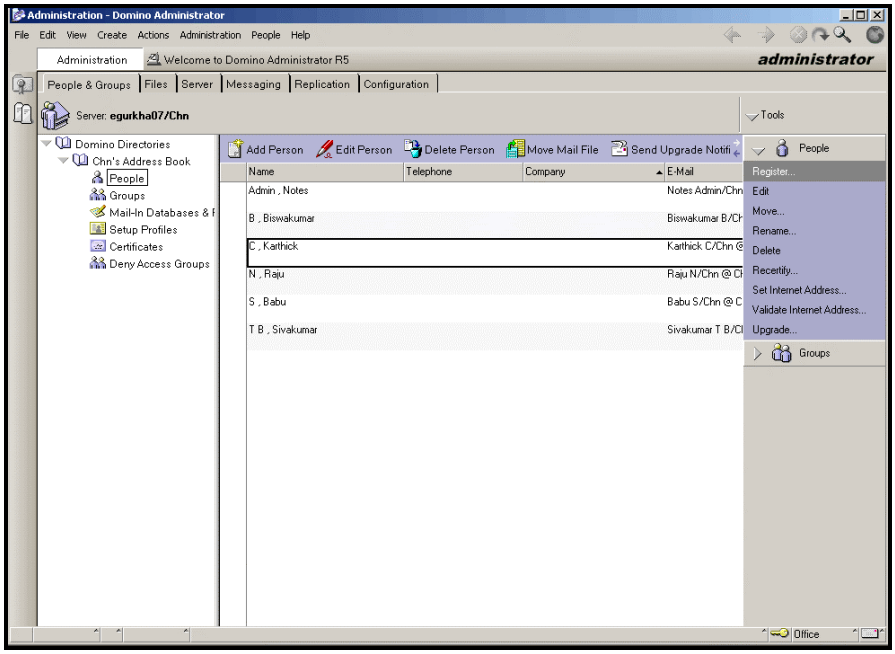

Figure 1.13: Selecting the Register option

- Upon selecting the **Register** option, Figure 1.14 appears wherein the details of the new user need to be provided.

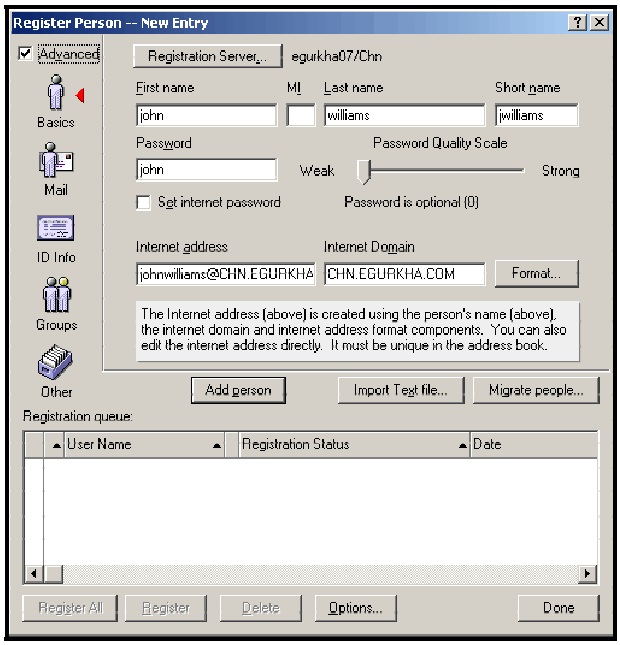

Figure 1.14: Adding the details of the new user

- After specifying the details, click on the **Add Person** button in Figure 1.14 to move the user specification to the **Registration queue** below (see Figure 1.15).

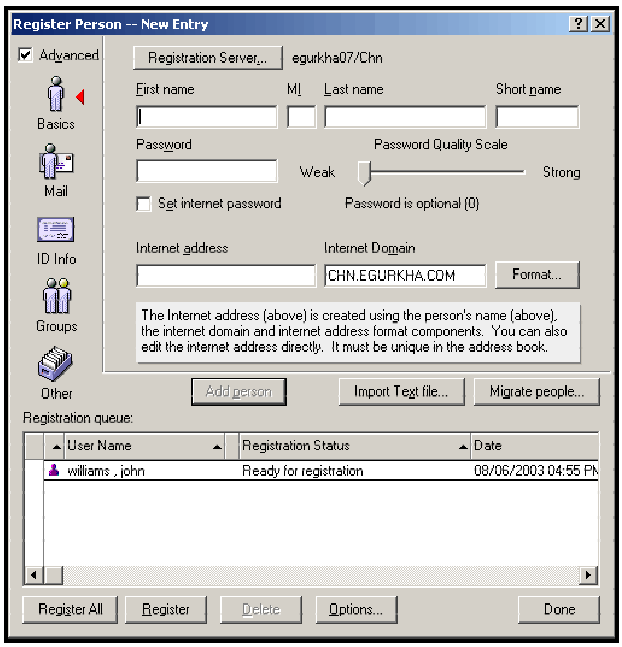

Figure 1.15: Adding the user to the Registration queue

- Now, click on the **Register** button in Figure 1.15 to register the details of the user in the queue.
- Once registration is complete, the added user will appear in the list of

users on the Domino mail server (see Figure 1.16).

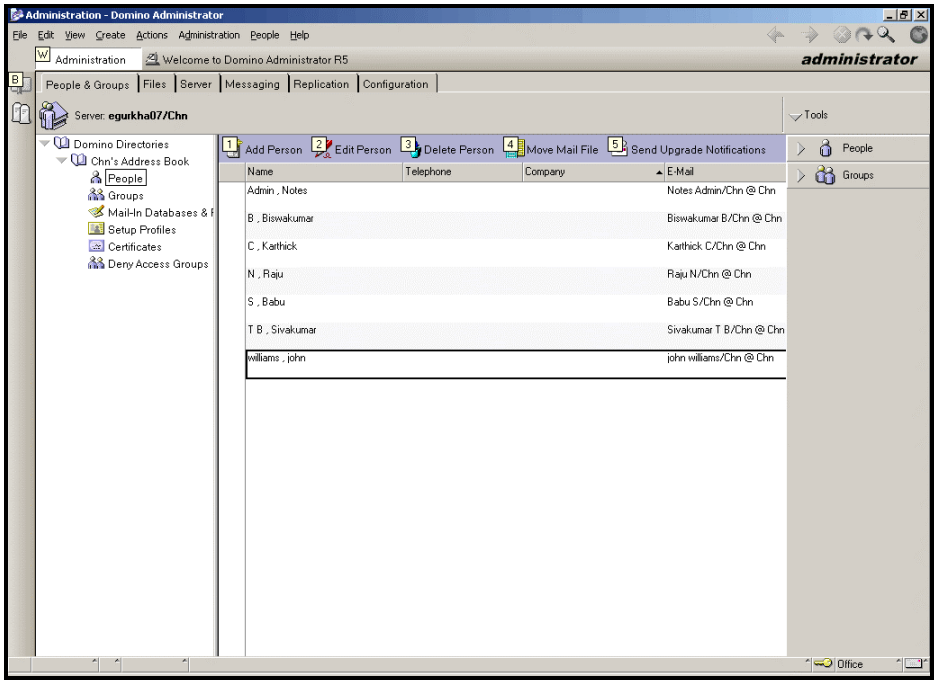
Administration - Domino Administrator
File Edit View Create Actions Administration People Help
Administration
Welcome to Domino Administrator R5
administrator
People & Groups Files Server Messaging Replication Configuration
Server: egurkha07/Chn
Tools
Domino Directories
Chn's Address Book
People
Groups
Mail-In Databases & F
Setup Profiles
Certificates
Deny Access Groups
1 Add Person 2 Edit Person 3 Delete Person 4 Move Mail File 5 Send Upgrade Notifications
People
Groups
Name Telephone Company E-Mail
Admin , Notes Notes Admin/Chn @ Chn
B , Biswakumar Biswakumar B/Chn @ Chn
C , Karthick Karthick C/Chn @ Chn
N , Raju Raju N/Chn @ Chn
S , Babu Babu S/Chn @ Chn
T B , Sivakumar Sivakumar T B/Chn @ Chn
williams , john john williams/Chn @ Chn
Office

Figure 1.16: The new user appears in the list of current users

- Double-click on the new user listing in Figure 1.16. Upon clicking, Figure 1.17 will appear wherein the specified details will appear. Below the specification, a certificate named **UserID** will be attached (see Figure 1.17), which contains all the user details.

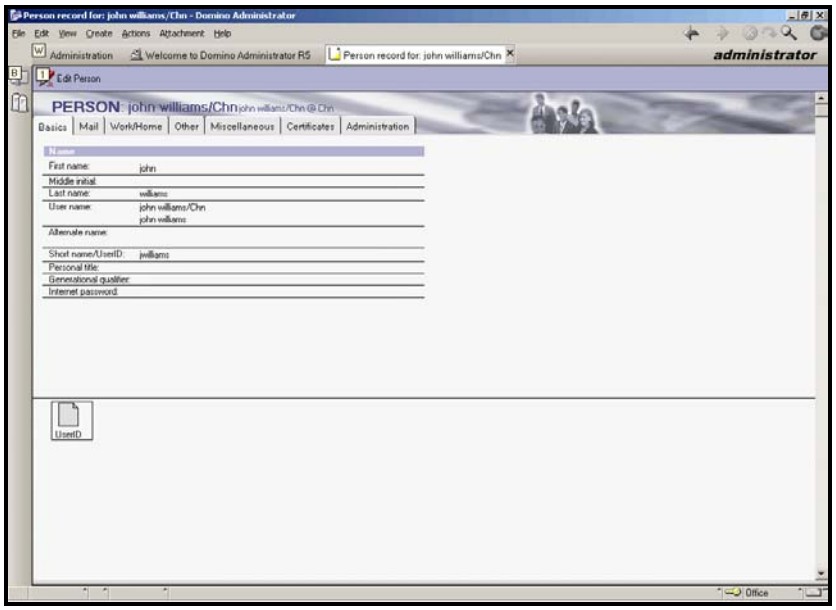

Figure 1.17: A screen displaying the details of the new user and a certificate

- While installing a Domino mail client, the installation process will

request for the Id/name of the user for whom the mailbox on the client is to be configured. During such circumstances, you either need to specify the name of a user or attach his/her certificate. When this is done, then such a user's mailbox will open by default, every time this user logs into the mail client. To facilitate easy identification, you can save the certificate in a more meaningful name. To do this, first, right-click on the certificate name in Figure 1.18, and select the **Detach** option (see Figure 1.18).

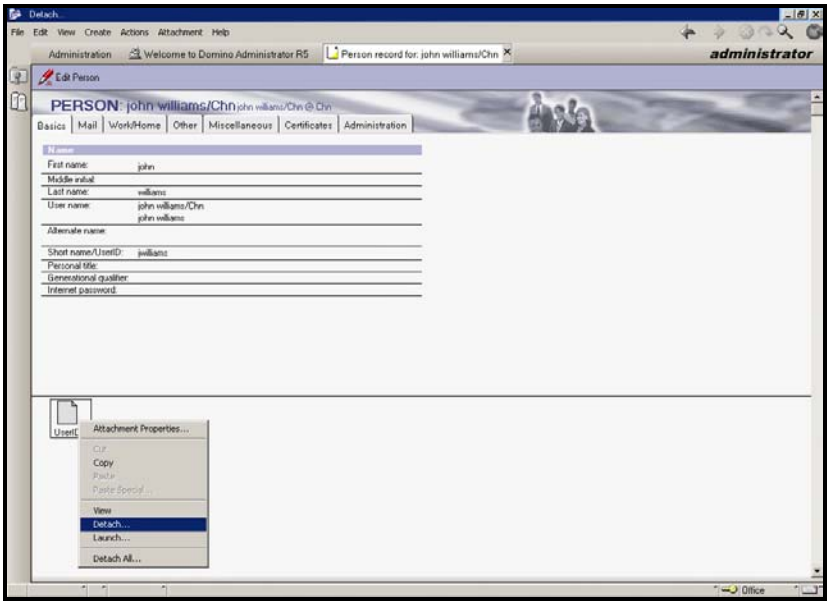

Figure 1.18: Detaching the certificate

- Figure 1.19 will appear wherein the current name of the certificate will be displayed in the **File name** text box. You can change it to read: **<username>.id** within double quotes, and then, click the **Detach** button.

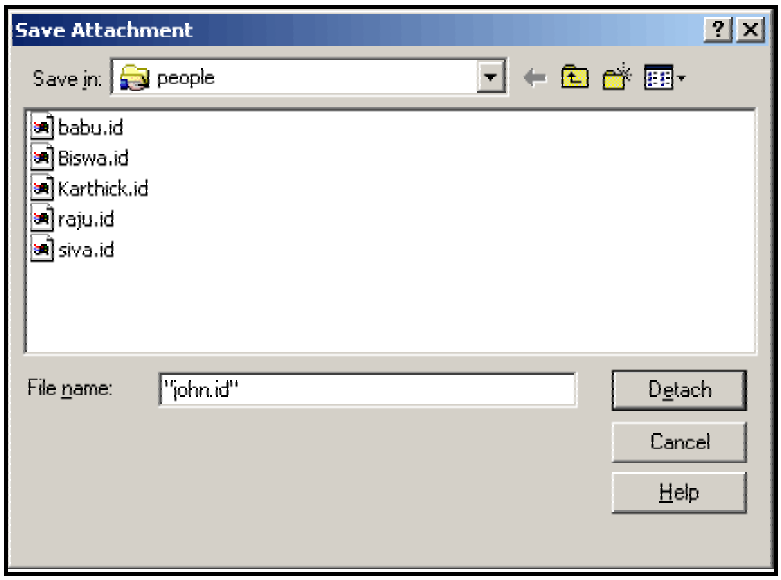

Figure 1.19: Changing the certificate name

Note:

- Notes client must be installed on the system where this test will be executed.
- This test will execute only on Windows environments.
- The **lcppn22.dll** is required by the user to run the DominoNrpcTest. To download this dll, do the following:
  - Connect to the URL:
    - http://www14.software.ibm.com/webapp/download/preconfig.jsp?id=2004-06-07+07%3A42%3A38.563764R&S_TACT=104AH%20W42&S_CMP=&s=
  - Download the **Lotus Notes C++ API Toolkit** in the URL to a location in your local disk.
  - An executable file (**.exe**) gets downloaded, which when executed, creates a **notescpp** directory in the specified location.
  - Also, an **lcppn22.dll** gets created within this **notescpp** directory.
  - Copy this **lcppn22.dll** to the **<LOTUS_NOTES_INSTALL_DIR>\notes** directory.

1.3 Administering the eG Manager to monitor the Lotus Domino Mail Server

After installation of the eG agent, please adhere to the following steps to configure the eG manager to monitor the Domino mail server.

1. Login to the eG user interface as an administrator.
2. Domino mail servers are referred to as the *Domino Mail* component type in the eG Enterprise system. If the Domino mail server is already discovered, use the Infrastructure -> Components -> Manage/Unmanage menu to manage it. Otherwise, run discovery to get the Domino mail Servers discovered (Infrastructure -> Components -> Discover) or manually add the Domino mail servers (Infrastructure -> Components -> Add/Modify). Adding components manually, will automatically render them "managed".
3. To manage the discovered components, go to the **Infrastructure -> Components -> Manage/Unmanage** page. The process of managing a component is clearly depicted by Figure 1.20 below.

For a more detailed procedure for managing components, refer to Configuring and Monitoring Web Servers document.

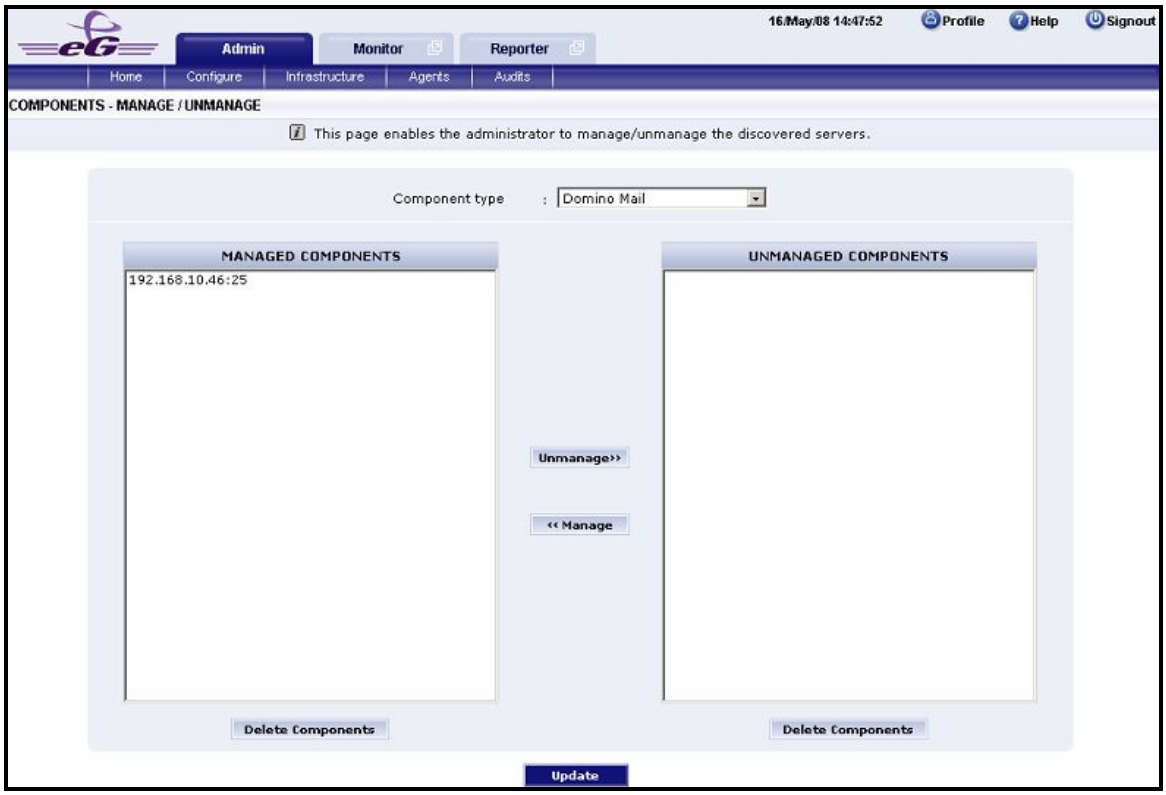

Figure 1.20: Managing a Domino Mail server

4. Now, on attempting to sign out, the following screen appears prompting users to configure the Domino Mail test and the Domino MailboxSize test. The Domino Mail test monitors the availability of the mail server from an external perspective. To do this, the Domino Mail test sends a test mail periodically from one user account to another and measures whether the mail was sent successfully and what the delivery time was. While the SMTP protocol is used to send mails, POP3 or IMAP protocols are used by the test to receive mails.

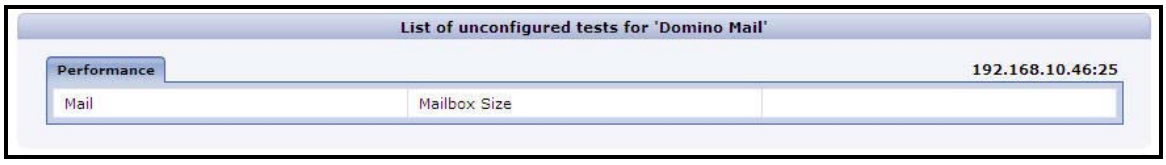

Figure 1.21: Viewing the tests to be configured for a Domino Mail server

5. Upon clicking the Mail test, a page depicted by Figure 1.22 will appear.

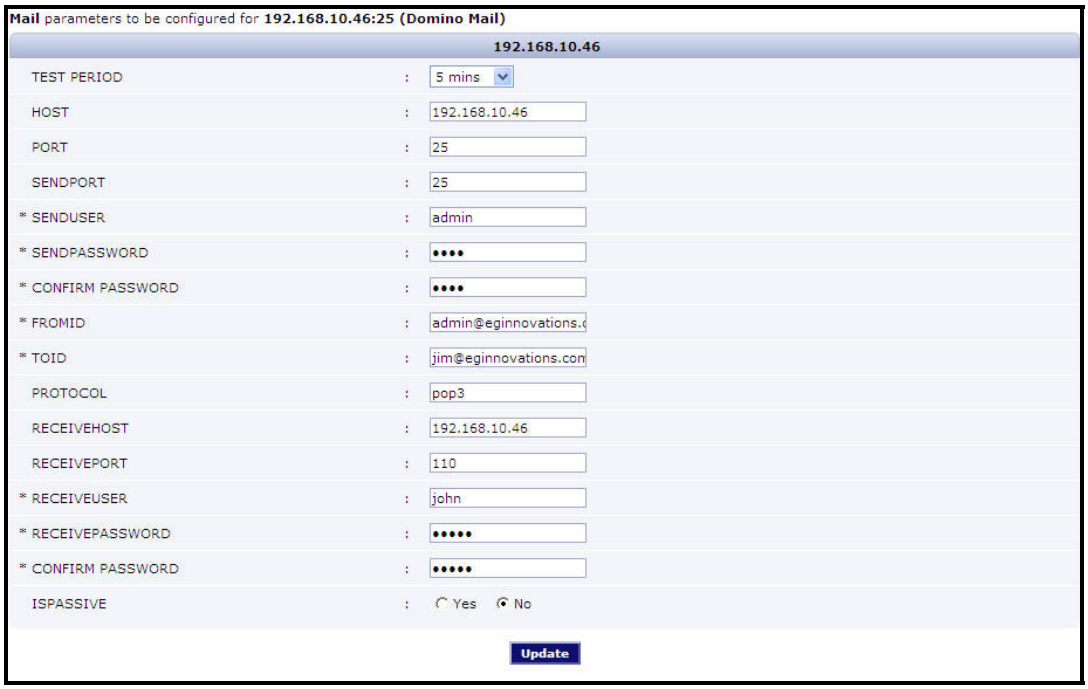

Figure 1.22: Configuring the test parameters for a Domino Mail server

6. In the parameters section of the page, configure the test parameters as follows:
   - **TEST PERIOD** - indicates how often this test needs to be executed.
   - **HOST** - indicates the IP address of the mail server
   - **PORT** - The port number of the mail server's routing engine
   - **SENDPORT** - The SMTP port of the mail server. The default SMTP port is 25.
   - **SENDUSER** - denotes the user name with which the test sends mails.
   - **SENDPASSWORD** - The password associated with the above user name. The **SENDUSER** and **SENDPASSWORD** can be 'none' if the target mail server does not need authentication to send mails.
   - **CONFIRM PASSWORD** – Confirm the **SENDPASSWORD** by retyping it here.
   - **FROMID** - takes the email id from which the test generates mails.
   - **TOID** - takes the email id to which the test sends mails. It is advisable that a separate email account be created for the MailTest.
   - **PROTOCOL** - The protocol to be used for receiving the mails (could be POP3 or IMAP).
   - **RECEIVEHOST** - indicates the IP address at which the test receives mails. Typically, this would be the IP address of a POP3 or IMAP server.
   - **RECEIVEPORT** - indicates the port number of the host, which receives the mails. The default port for POP3 is 110 and that of IMAP is 143.
   - **RECEIVEUSER** - indicates the user name with which the test receives mails.
   - **RECEIVEPASSWORD** - indicates the password corresponding to the above user.
   - **CONFIRM PASSWORD** – Confirm the **RECEIVEPASSWORD** by retyping it here.
   - **ISPASSIVE** - In the case of Exchange 2000 servers, the MailTest takes an additional

ISPASSIVE parameter. If the value chosen against this parameter is **YES**, then the Exchange server under consideration is a passive server in an Exchange cluster. No alerts will be generated if the server is not running. Measures will be reported as "Not applicable' by the agent if the server is not up. This Parameter is applicable to Exchange 2000 servers only, though it appears in the **MailTest** configuration pages of MS Exchange 5.5 and Lotus Domino servers.

Here are example settings of the Mail test parameters:

a. **SENDPORT** = 25
b. **SENDUSER** = none
c. **SENDPASSWORD** = none
d. **FROMID** = mailto:mailtest@test.com
e. **TOID** = mailtest@test.com
f. **PROTOCOL** = POP3
g. **RECEIVEHOST** = mail.test.com (the POP3 server's host)
h. **RECEIVEPORT** = 110
i. **RECEIVEUSER** = mailtest
j. **RECEIVEPASSWORD** = mailtest's password

It is advisable that you create a separate user account on your mail server for this test to use.

7. Attempting to signout again will bring up the **LIST OF UNCONFIGURED TESTS** once again, but this time it will prompt you to configure the Mailbox Size test. Doing so will open Figure 1.23.

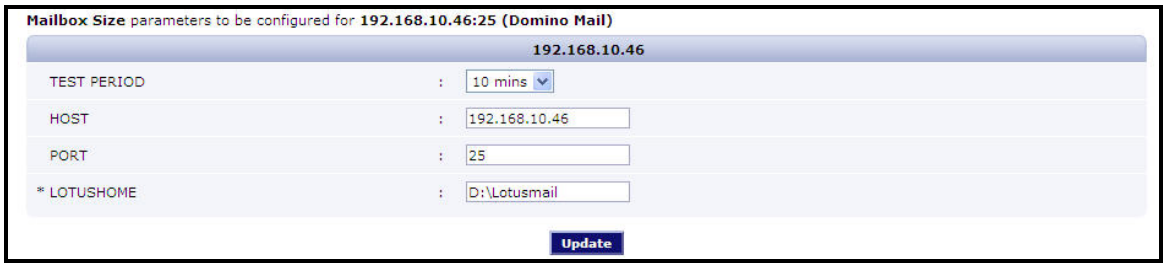

Figure 1.23: Configuring the Mailbox Size test

8. Here, specify the following:
   - **TESTPERIOD** - How often should the test be executed
   - **HOST** –The host for which the test is to be configured.
   - **PORT** – The port number of the Domino mail server.
   - **LOTUSHOME** – The install directory of Lotus Notes.

9. Finally, click the **Update** button in Figure 1.23.
10. The NRPC test reports whether a Notes client is able to connect to the Lotus Domino mail server, and also measures the responsiveness of the mail server. This test is disabled by default.
11. To enable this test use the menu sequence **Agents** -> **Tests** -> **Enable/Disable.** An administrator has to first choose the type of component (from the **Component type** list box) and the type of test (from the **Test type** list box) for which the tests have to be either enabled or disabled. Remember that the **Select a component type** list box lists only those component-types that have been managed by eG Enterprise.

> **Note:**
>
> This test will report measures only if the following are in place:
>
> - The Domino HTTP Server should be running.
> - The DIIOP task of the Domino mail server should have been started.
> - The **NCSO.jar** file available in the **<LOTUSNOTES_INSTALL_DIR>\Domino\Data\domino\java** directory should be copied to the <**EG_INSTALL_DIR>\lib** directory.

12. Figure 1.24 depicts the complete list of performance tests that are enabled and disabled by default for the chosen Domino Mail component type. To enable the test open the **ENABLE-DISABLE TESTS** page by following the menu sequence *Agents* -> *Tests* -> *Enable/Disable*. In this page, you can either preclude or exclude a test from being executed for a specific a test type of a component type.
13. For an example, to preclude any of the performance tests of Domino Mail component type, select the desired options from the drop-down list as depicted by the figure. Now select the test names from the **DISABLED TESTS** list box and click on the **<<** button. (see Figure 1.24).

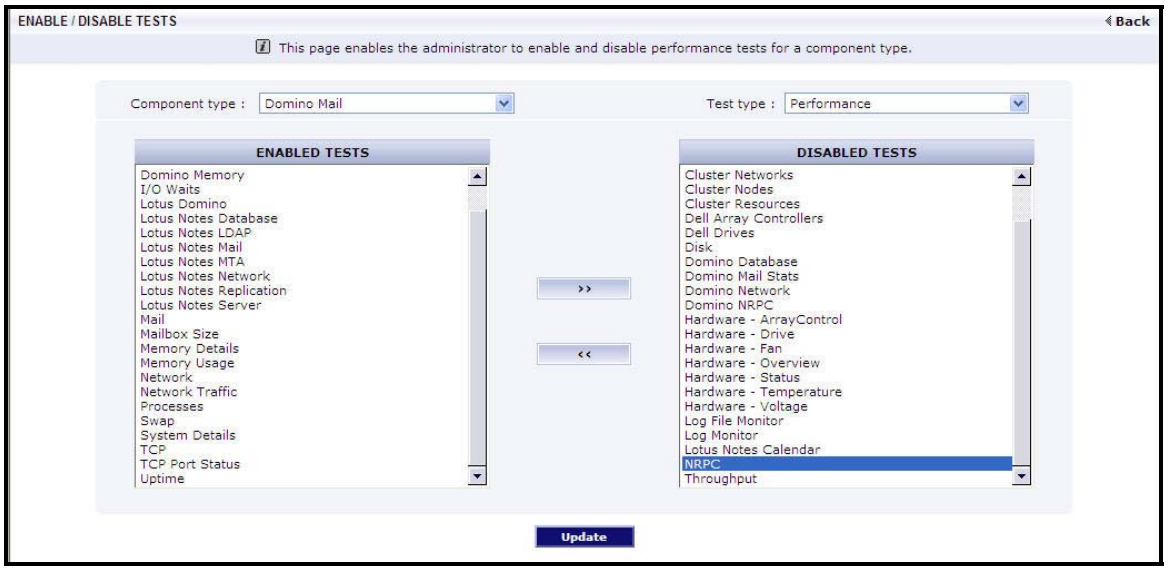

Figure 1.24: Selecting the tests to be enabled for Domino Mail server

14. Figure 1.25 depicts the chosen tests of Domino Mail server have been included in the **ENABLED TESTS** list box. Click on **Update** button to implement the changes.

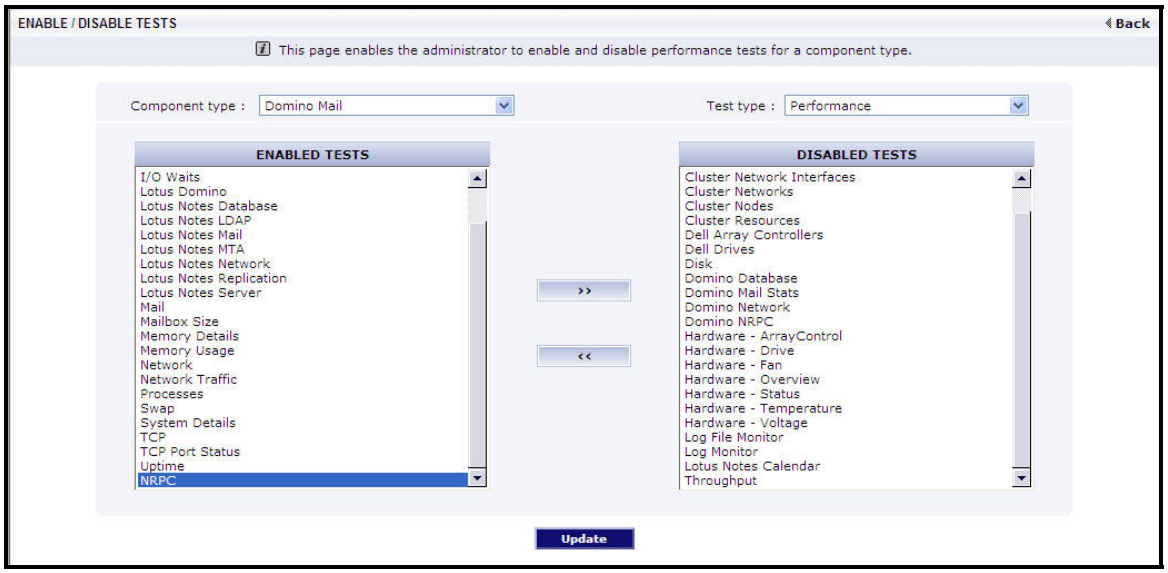

Figure 1.25: Enabling the tests for the Domino Mail server

Note:

This test will report measures only if the following are in place:

The Domino HTTP Server should be running.

The DIIOP task of the Domino mail server should have been started.

The **NCSO.jar** file available in the **<LOTUSNOTES_INSTALL_DIR>\Domino\Data\domino\java** directory should be copied to the <**EG_INSTALL_DIR>\lib** directory.

15. Then, return to the **AGENTS – TESTS SPECIFIC CONFIGURATION** page using the menu sequence **Agents** -> **Tests** -> **Configure** -> **Specific**.
16. First choose Domino Mail from the **Component type** list box and the specific component from the **Component name** list box. Then choose type of a test say as Performance from the **Test type** list box. Doing so will provide the agent summary details and as well the configuration status of all the tests pertaining to the chosen component respectively.

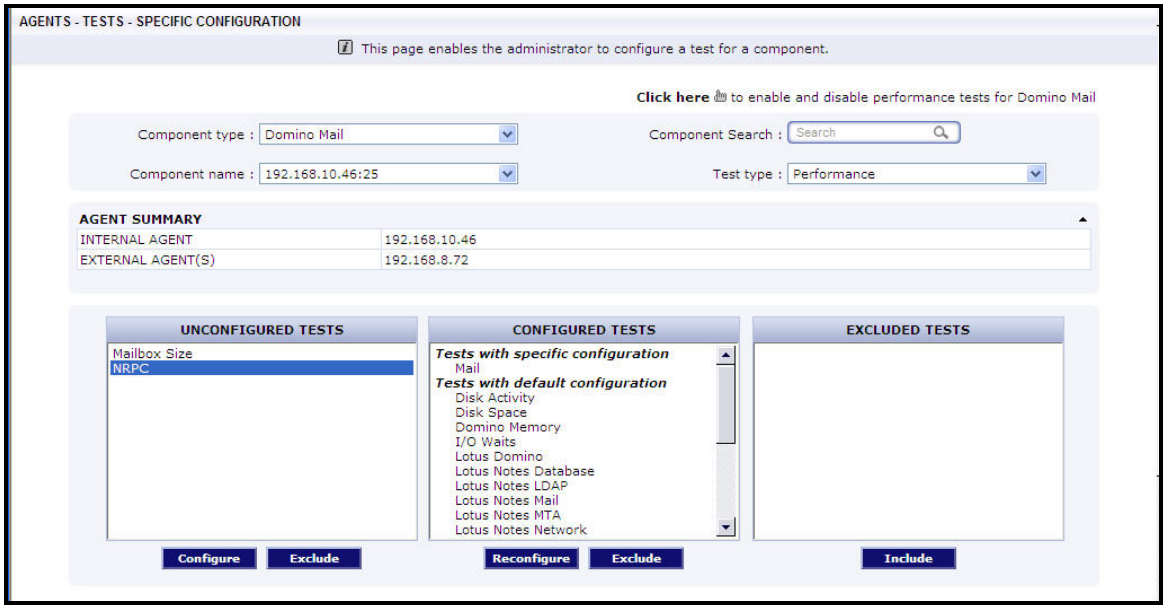

Figure 1.26: Selecting NRPC test from the unconfigured tests

17. To configure an unconfigured test, select the NRPC test from the **UNCONFIGURED TESTS** list box and click on the **Configure** button. This will invoke the parameters to be configured for the chosen test. Finally click on the **Update** button to implement the changes as depicted by the Figure 1.27.

18. Upon clicking, the test parameters will be displayed (see Figure 1.27):
    a. **TEST PERIOD** - How often should the test be executed
    b. **HOST** - The IP address of the machine where the Domino server is installed.
    c. **PORT** – The port number through which the Domino mail server

communicates

d. **HTTPPORT** – The port of the Domino HTTP server.

e. **USERNAME** – The user name using which the test needs to connect to the Domino mail server.

f. **PASSWORD** – The password of the specified **USERNAME**.

g. **CONFIRM PASSWORD** – Confirm the password by retyping it here.

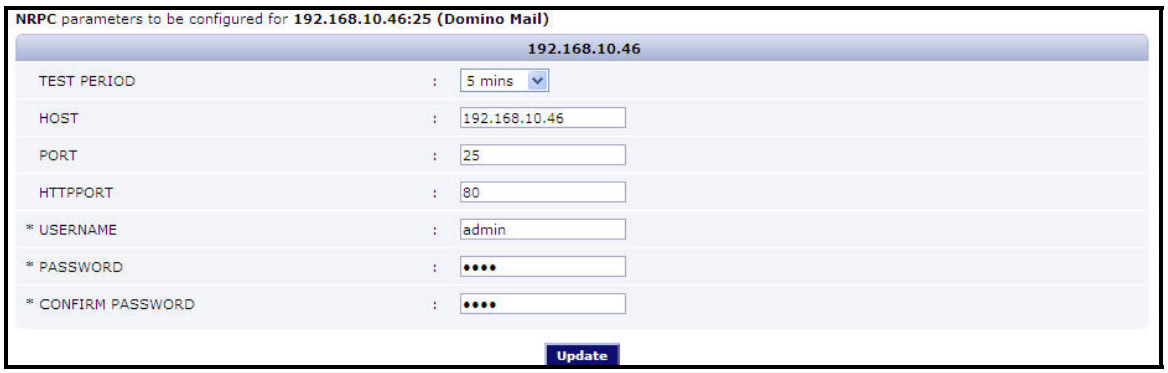

Figure 1.27: Configuring the NRPC test

19. Finally, click on the **Update** button to register the changes.

1.4 Monitoring the Lotus Domino Mail Server

To view the measurements collected during monitoring, do the following:

1. Login as a monitor / supermonitor user via the eG user interface.
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. From the displayed independent components list, click the *Domino Mail* server. The layer model of the Domino mail server will then appear. Click on a layer to view the tests mapped to it, and click on a test to view the corresponding measures.
4. You can also view a graph of the measurements and history of the measurements, and can also record the details of action taken to fix errors.
5. Once you are done viewing the measurements, just click on the **Signout** option.

Chapter 2

Configuring and Monitoring an MS Exchange Server

This chapter deals with the following:

- Configuring an MS Exchange Server
- Administering the eG manager to monitor an MS Exchange server
- Monitoring the MS Exchange server

2.1 Configuring an MS Exchange Server 5.5 to work with the eG Manager

The MsXMail test, which is executed by an eG external agent, mimics an MS Outlook mail client that sends and receives mails from an Exchange server. Whereas eG Enterprise's Mail test relies on SMTP and POP3/IMAP protocols to communicate with the mail server, the MsXMailTest is used for emulating client accesses via the native Microsoft Mail protocol (i.e. in situations where SMTP/POP3/IMAP are not enabled for a mail server). This test takes three main parameters:

- A user mailbox that the test uses to send and receive mails
- The site on the Exchange server that hosts this user account
- The organizational unit on the Exchange server that hosts this site

In order to ensure that this test functions, the following conditions are to be fulfilled:

- The eG external agent that is executing the MsXMailTest, should be installed on a Windows NT server/client in the same domain as the MS Exchange server.
- The administrator configuring the test should ensure that the mailbox being used in the test, exists on the Exchange server. If no mailboxes exist, then follow the instructions given below to create one for an existing Windows NT domain user:

    a. Click the **Start** button on the task bar of the Windows NT server that hosts the Exchange server, and follow the menu sequence: Start -> Programs -> Microsoft Exchange Server -> Microsoft Exchange Administrator (see Figure 2.1):

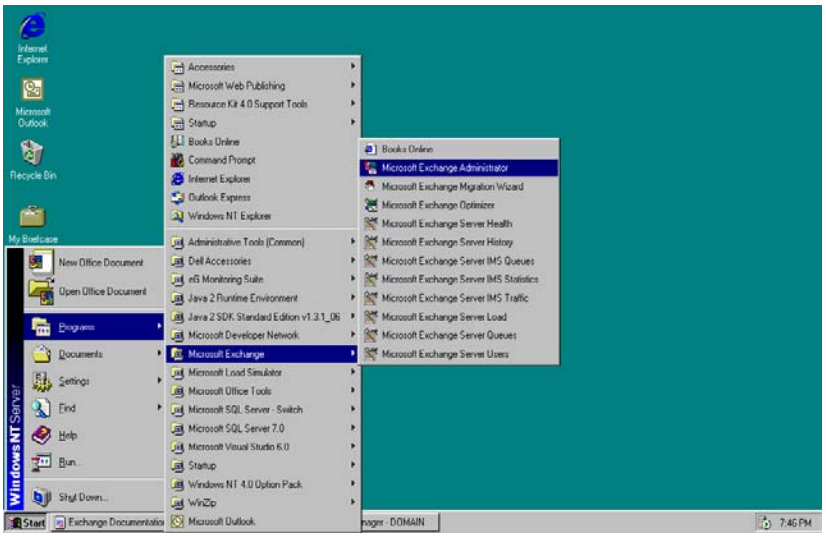

Figure 2.1: The Microsoft Exchange Administrator window

Note:

Administrator privileges are required for creating a mailbox on the MS Exchange server 5.5

b. The administrator window that appears has a tree structure in its left pane (Figure 2.2). The top-most node of the tree structure is the organizational unit on the Exchange server. Expanding this node, reveals the complete list of sites in the organization. Expanding a site, reveals a **Recipients** sub-node, clicking on which, the existing user accounts (mailboxes) on the site will be displayed in the right pane (see Figure 2.2).

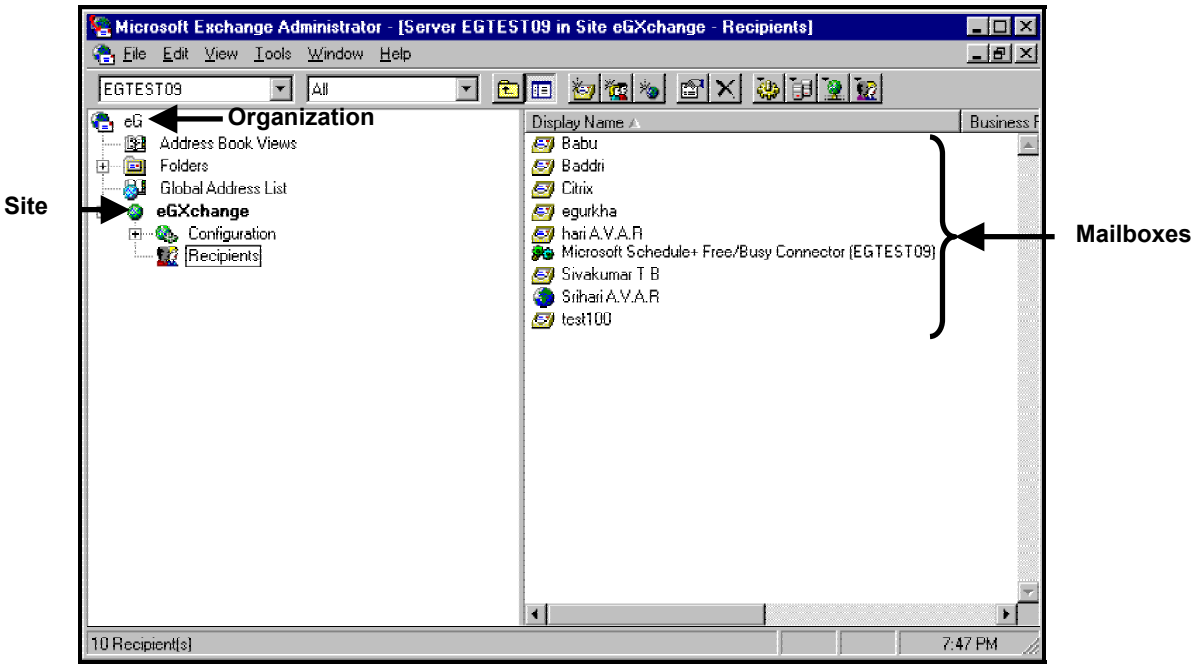

Figure 2.2: The Administrator window

c. Next, select the site on which the mailbox is to be created, click on the **File** option on the menu bar, and select **New Mailbox**, to create a new mail box on the selected site (see Figure 2.3).

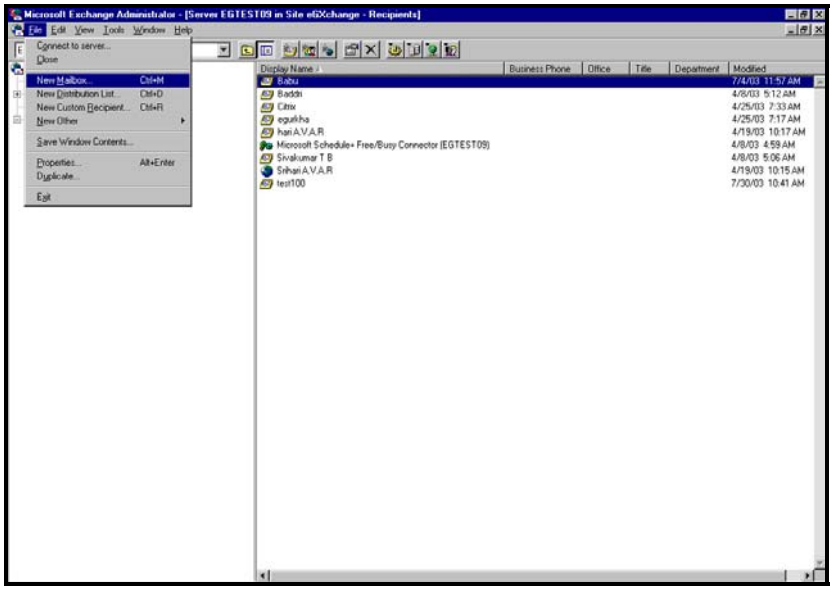

Figure 2.3: Creating a mailbox for a user

d. In the **Properties** dialog box that appears (see Figure 2.4), specify the details of the user's mailbox. If the Windows NT user account which is to be associated with the new mailbox already exists in the same domain as the MS Exchange server, then that user account will be automatically displayed against **Primary Windows NT Account** (see Figure 2.4). However,

such an automatic association is possible only if the name of the user account and the mailbox are the same. If not, you can click on the **Primary Windows NT Account** button to explicitly define the association.

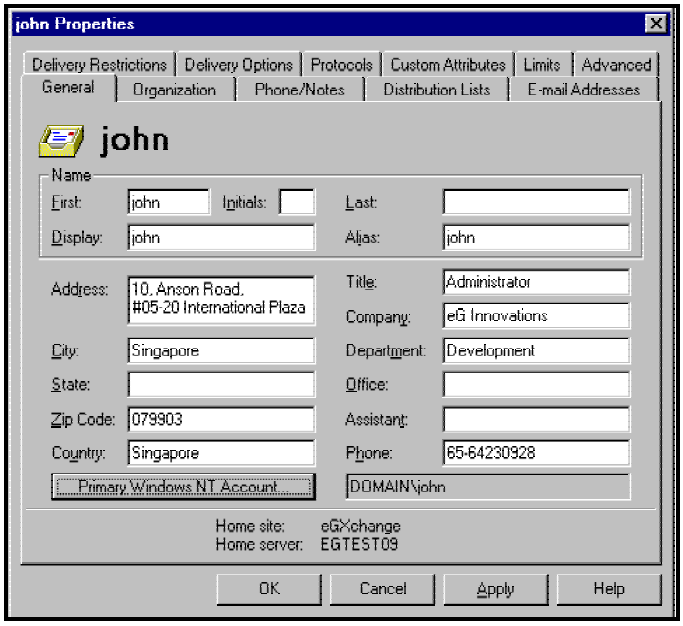

Figure 2.4: Specifying the details of the new user account

e. Finally, click the **Apply** button in Figure 2.4 to register the changes, and then, click the **OK** button to close the dialog box.

f. Once back in the Exchange Administrator window (see Figure 2.5), drill-down the tree structure in the left pane using the following node-sequence: <Organization name> -> <Site name> -> Recipients (see Figure 2.5). This will display the list of mailboxes in the right pane. Note that the newly created mailbox is listed therein (see Figure 2.5).

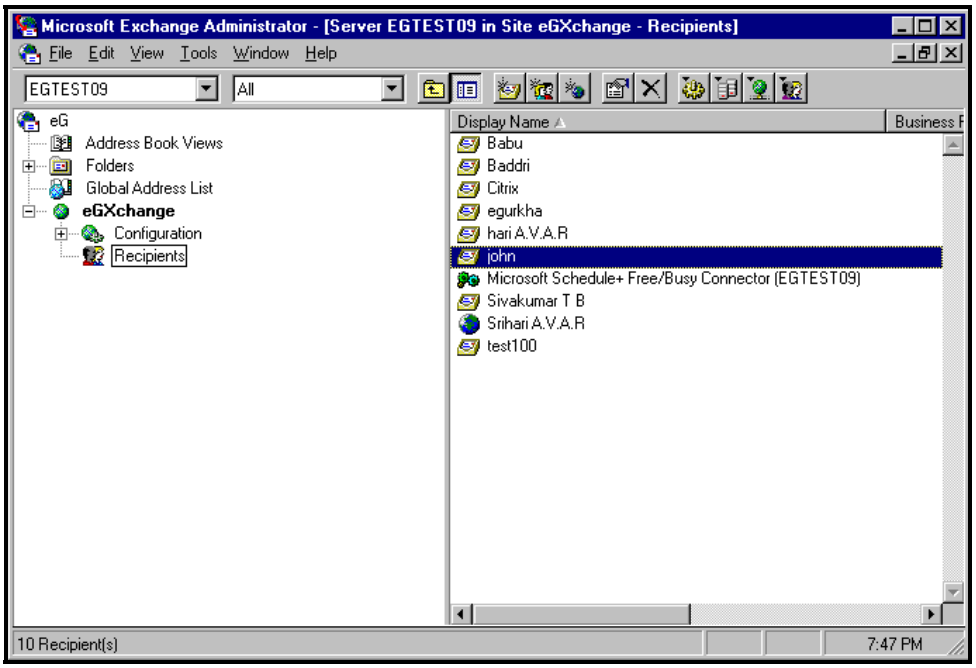

Figure 2.5: The newly created mailbox being displayed in the Administrator window

- The eGurkhaAgent service should run using the NT account information of the user whose mailbox has been configured for the MsXMail test
- By default, the eGurkhaAgent service uses the LocalSystem account for execution. This account however, may not permit an external agent to access the mailbox that has been configured for the MsXMail test. Hence, the eGurkhaAgent service should be made to run using the login information of the user whose mailbox has been configured for the MsXMail test.
- For example, assume that the administrator has decided to use the Windows NT user *john's* mail box for configuring the MsXMail test. To login to a Windows NT server/client, *john* uses the user name *john* and the password *john*. To ensure that the external agent gains access to *john's* mailbox for monitoring, the above-mentioned login information should be passed to the eGurkhaAgent service.
- To achieve this, do the following:

    a. Login to the Windows NT server hosting the external agent as an eG user who has a mailbox on the Exchange server 5.5.

    b. Then, open the **Services** window of the server (see Figure 2.6) using the menu sequence: Start -> Programs -> Administrative Tools -> Services.

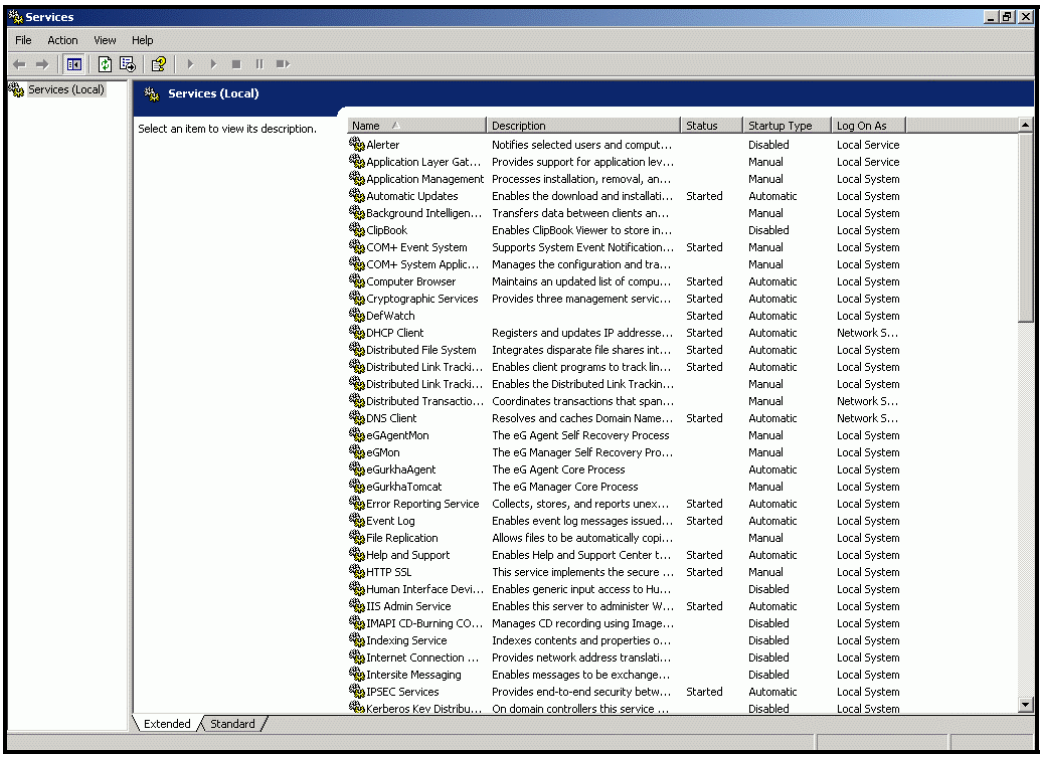
Services
File Action View Help
Services (Local)
Services (Local)
Select an item to view its description.
Name Description Status Startup Type Log On As
Alerter Notifies selected users and comput... Disabled Local Service
Application Layer Gat... Provides support for application lev... Manual Local Service
Application Management Processes installation, removal, an... Manual Local System
Automatic Updates Enables the download and installati... Started Automatic Local System
Background Intelligen... Transfers data between clients an... Manual Local System
ClipBook Enables ClipBook Viewer to store in... Disabled Local System
COM+ Event System Supports System Event Notification... Started Manual Local System
COM+ System Applic... Manages the configuration and tra... Manual Local System
Computer Browser Maintains an updated list of compu... Started Automatic Local System
Cryptographic Services Provides three management servic... Started Automatic Local System
DefWatch Started Automatic Local System
DHCP Client Registers and updates IP addresse... Started Automatic Network S...
Distributed File System Integrates disparate file shares int... Started Automatic Local System
Distributed Link Tracki... Enables client programs to track lin... Started Automatic Local System
Distributed Link Tracki... Enables the Distributed Link Trackin... Manual Local System
Distributed Transactio... Coordinates transactions that span... Manual Network S...
DNS Client Resolves and caches Domain Name... Started Automatic Network S...
eGAgentMon The eG Agent Self Recovery Process Manual Local System
eGMon The eG Manager Self Recovery Pro... Manual Local System
eGurkhaAgent The eG Agent Core Process Automatic Local System
eGurkhaTomcat The eG Manager Core Process Manual Local System
Error Reporting Service Collects, stores, and reports unex... Started Automatic Local System
Event Log Enables event log messages issued... Started Automatic Local System
File Replication Allows files to be automatically copi... Manual Local System
Help and Support Enables Help and Support Center t... Started Automatic Local System
HTTP SSL This service implements the secure ... Started Manual Local System
Human Interface Devi... Enables generic input access to Hu... Disabled Local System
IIS Admin Service Enables this server to administer W... Started Automatic Local System
IMAPI CD-Burning CO... Manages CD recording using Image... Disabled Local System
Indexing Service Indexes contents and properties o... Disabled Local System
Internet Connection ... Provides network address translati... Disabled Local System
Intersite Messaging Enables messages to be exchange... Disabled Local System
IPSEC Services Provides end-to-end security betw... Started Automatic Local System
Kerberos Key Distribu... On domain controllers this service ... Disabled Local System
Extended Standard

Figure 2.6: The Services window displaying the eGurkhaAgent service

c. Double-click on the eGurkhaAgent service in Figure 2.6 to open its **Properties** (see Figure 2.7) dialog box. Click on the **Log On** tab of the dialog box (see Figure 2.7), select the **This Account** option, and specify the name of user whose mailbox is to be configured. Then, specify the **Password** of the user and confirm it by retyping it in the **Confirm Password** text box. This name and password should be the same as those specified while creating the user on Windows NT. The **Browse** button can also be used to specify the user name (see Figure 2.7).

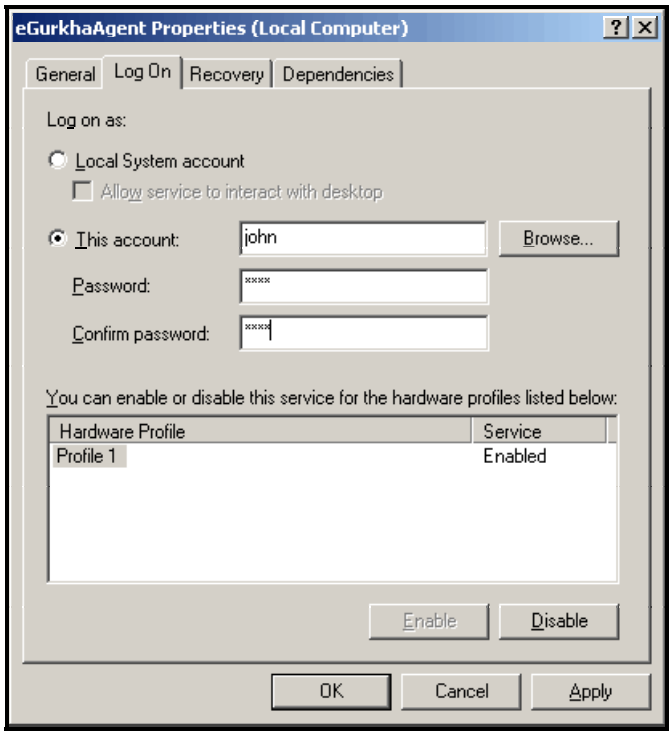

Figure 2.7: Configuring the eGurkhaAgent service to use the eG user name

d. Finally, click on the **Apply** button in Figure 2.7, followed by the **OK** button.

2.2 Administering the eG Manager to monitor an MS Exchange 5.5 Server

After installation of the eG agent, follow the following steps to configure eG to monitor MS Exchange servers (version 5.5 and 2000).

1. Login to eG user interface as an administrative user.
2. eG monitors MS Exchange Server 5.5 and MS Exchange Server 2000 as two different server types. If the MS Exchange Server 5.5 (referred to as *Exchange 5.5* the eG Enterprise system) is already discovered, use the menu sequence Infrastructure-> Components -> Manage/Unmanage to manage it. The screens below depict the process of managing an Exchange 5.5 server clearly.

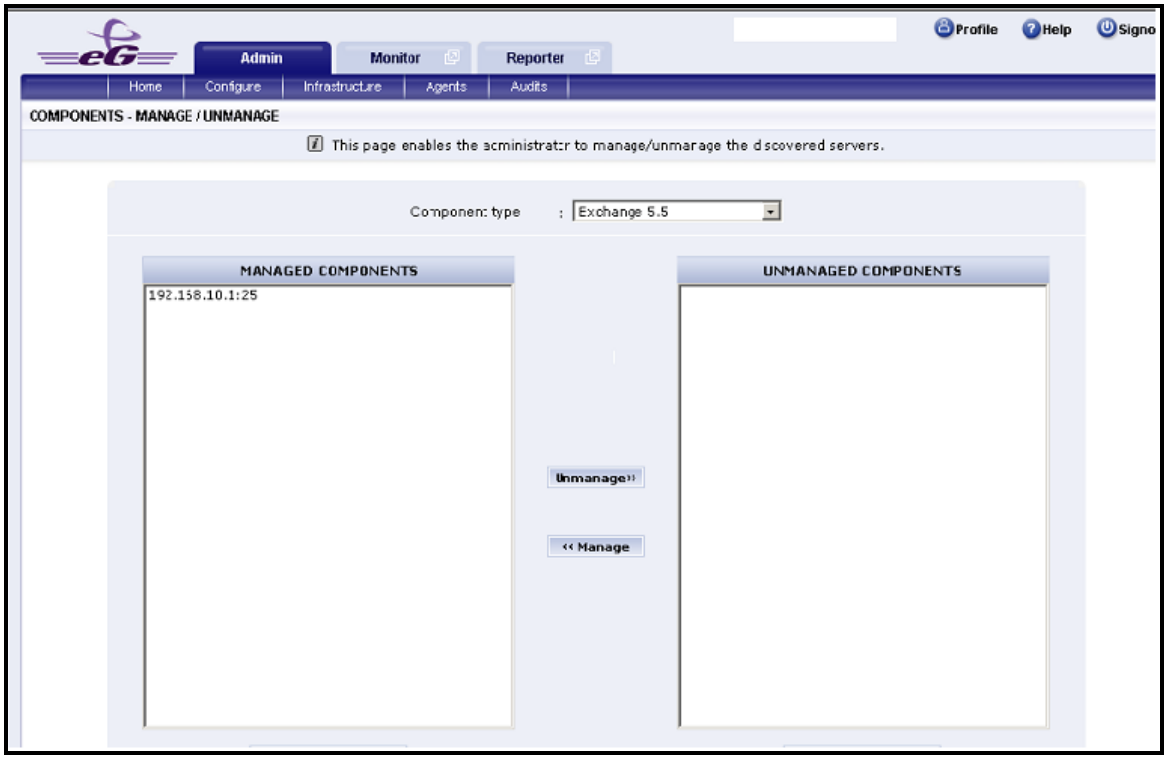

Figure 2.8: Managing an Exchange 5.5 server

3. On the other hand, if the component is not discovered, run discovery to get the Exchange servers discovered or manually add them. Proceed to manage discovered components as discussed above. Components manually added, are however, automatically managed.

Refer

Please refer to Configuring and Monitoring Web Servers document for a more elaborate discussion on how to discover components, add them manually and manage them.

4. Once again, on signing out, you would be prompted to configure the Exchange 5.5 Mail test. However, if the Exchange Mail test is already configured (for eg., while configuring an Exchange 5.5 mail server), then no such prompt will appear.

Refer

Please refer to Chapter 1.1 above for a more elaborate discussion on how to configure the Mail test

The MsXMail test emulates a client connecting to a Microsoft Exchange server and sending/receiving mails. The eG Enterprise system, by default, switches off the execution of the MsXMail test. An administrator can optionally turn this test on, so that it can be executed on the Exchange 5.5 server. Figure 2.9 depicts the complete list of performance tests that are enabled and disabled by default for the chosen exchange 5.5 component

type. To enable the test open the **ENABLE-DISABLE TESTS** page by following the menu sequence *Agents* -> *Tests* -> *Enable/Disable*. In this page, you can either preclude or exclude a test from being executed for a specific a test type of a component type.

For an example, to preclude any of the performance tests of Exchange 5.5 component type, select the desired option from the drop-down list as depicted by the figure. Now select the test names from the **DISABLED TESTS** list box and click on the **<<** button. (see Figure 2.9).

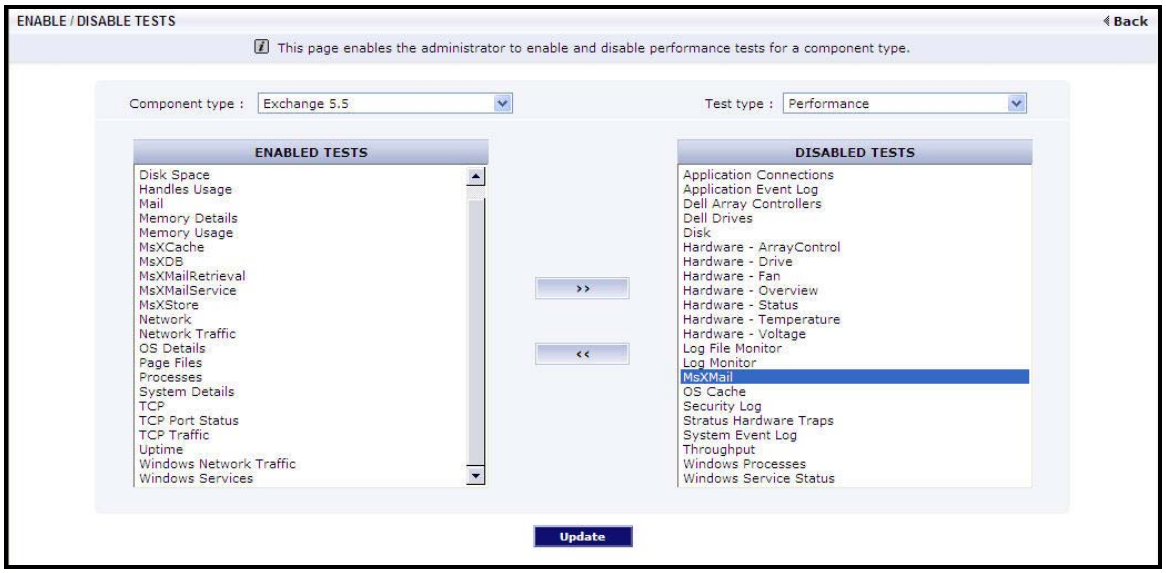

Figure 2.9: Selecting the tests to be enabled for Exchange 5.5 component type

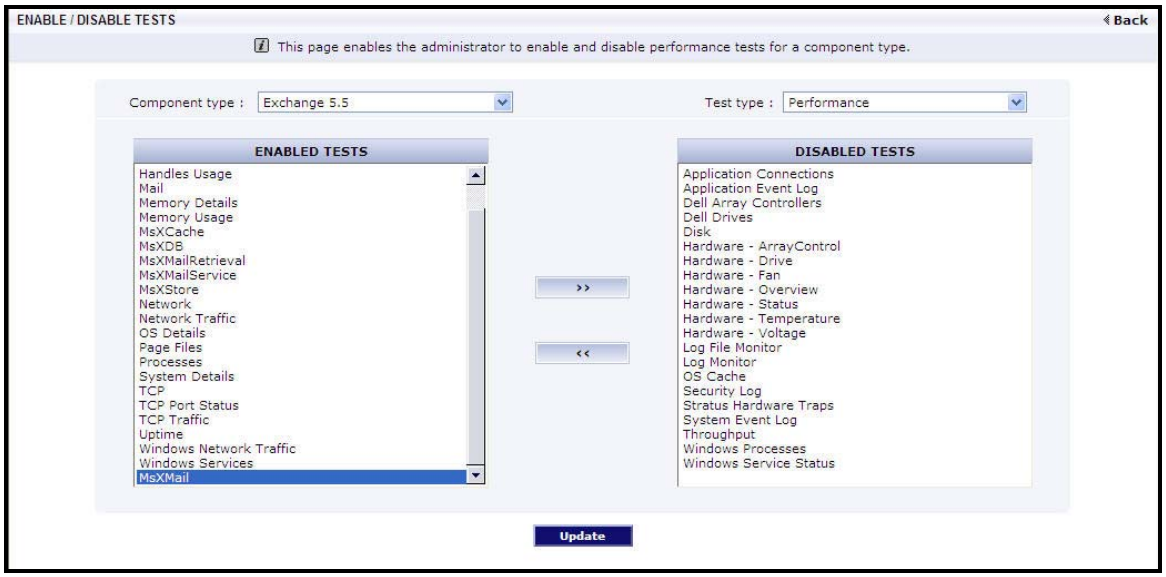

Figure 2.10: Enabling the tests for the Exchange 5.5 component type

Then, return to the **AGENTS – TESTS SPECIFIC CONFIGURATION** page using the menu sequence **Agents** -> **Tests** -> **Configure** -> **Specific**.

First choose Exchange 5.5 from the **Component type** list box and the specific component from the **Component name** list box. Then choose type of a test say as Performance from the **Test type** list box. Doing so will provide the agent summary details and as well the configuration status of all the tests pertaining to the chosen component respectively.

To configure an unconfigured test, select the MsxMail test from the **UNCONFIGURED TESTS** list box and click on the **Configure** button. This will invoke the parameters to be configured for the chosen test. Finally click on the Update button to implement the changes as depicted by the Figure 2.10.

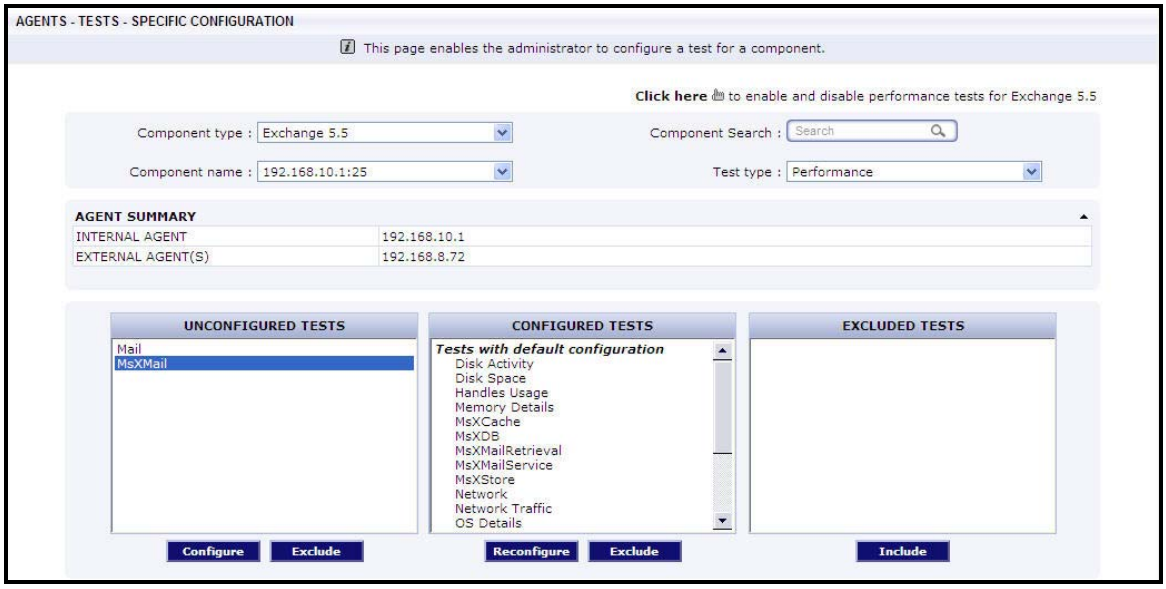

Figure 2.11: Selecting MsxMail test from the unconfigured tests

5. Upon clicking, the test parameters will be displayed (see Figure 2.12):
   - **TEST PERIOD** - How often should the test be executed
   - **HOST** - The IP address of the machine where the Exchange 5.5 server is installed.
   - **PORT** – The port number through which the Exchange 5.5 server communicates. The default port number is 25.
   - **XCHGMAILBOX** - Specify the user name or the user ID of a user mail box available on the Exchange server that is to be used for this test.
   - **XCHGSITENAME** - The name of a site in the Exchange server
   - **XCHGORGNAME** - The name of the organization in the Exchange server to which the specified site belongs

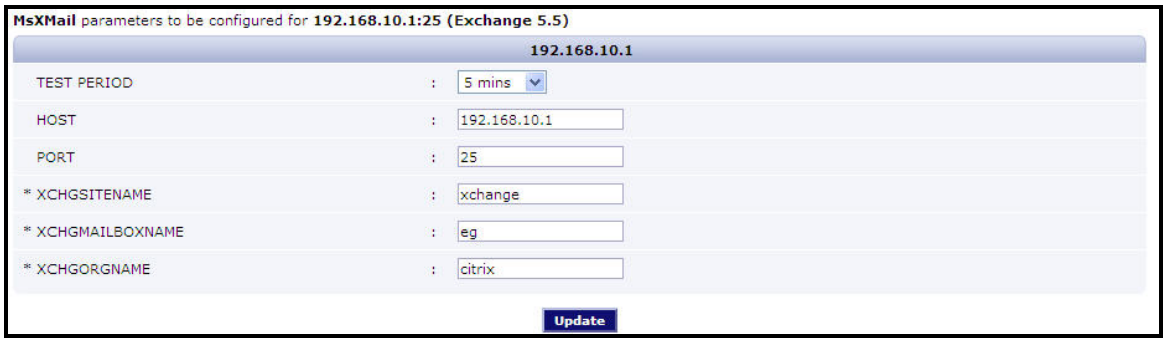

Figure 2.12: Configuring the MsXMail test

6. Finally, click the **Update** button in Figure 2.12.
7. Once you are done with the configuring, sign out of the administrative interface.
8. Then, start the eG agent on the system that is hosting the Exchange server.

2.3 Monitoring the MS Exchange 5.5 Server

1. Login to the monitor user interface of an *Exchange 5.5* server.
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. View the *Exchange 5.5* Server in the independent components list and click on it to view its layer model, tests, and measurements.

Chapter 3

Configuring and Monitoring an Exchange 2000/2003 Server

This chapter deals with the following:

- Configuring an Exchange 2000/2003 server
- Administering the eG manager to monitor an Exchange 2000/2003 server
- Monitoring the Exchange 2000/2003 server

3.1 Configuring an Exchange Server 2000/2003 to work with the eG Manager

The XchgMail test, which is executed by an eG external agent, mimics an MS Outlook mail client that sent and receives mails from an Exchange server. Whereas eG Enterprise's Mail test relies on SMTP and POP3/IMAP protocols to communicate with the mail server, the XchgMail test is used for emulating client accesses via the native Microsoft Mail protocol (i.e. in situations where SMTP/POP3/IMAP are not enabled for a mail server). This test takes two main parameters:

- A email ID of the user mailbox that the test uses to send and receive mails
- The Profile that is used by the configured user mailbox

In order to ensure that this test functions, the following conditions are to be fulfilled:

- The eG external agent that is executing the XchgMail test, should be installed on a Windows 2000 (or 2003) server/client in the same domain as the Exchange 2000/2003 server.
- This test uses only a Microsoft Outlook 2003 client for sending/receiving mails from the server. **Note that the XchgMail test will not work with Microsoft Outlook Client 2000/2002.**
- The Microsoft Outlook 2003 client used by the test should have been installed with the **Collaboration Data Objects** option enabled; to know how to modify your Outlook installation to enable this option, refer to Section 3.4 of this manual.
- The administrator configuring the test should ensure that the email ID being used in the test, exists on the Exchange 2000/2003 server. If it does not exist, then follow the instructions given below to create a mailbox (these instructions are specific to an Exchange 2000 server) and an email ID that corresponds to it:

a. Click the **Start** button on the task bar of the Windows 2000 server, and follow the menu sequence: Start -> Programs -> Microsoft Exchange -> Active Directory Users and Computers (see Figure 3.1):

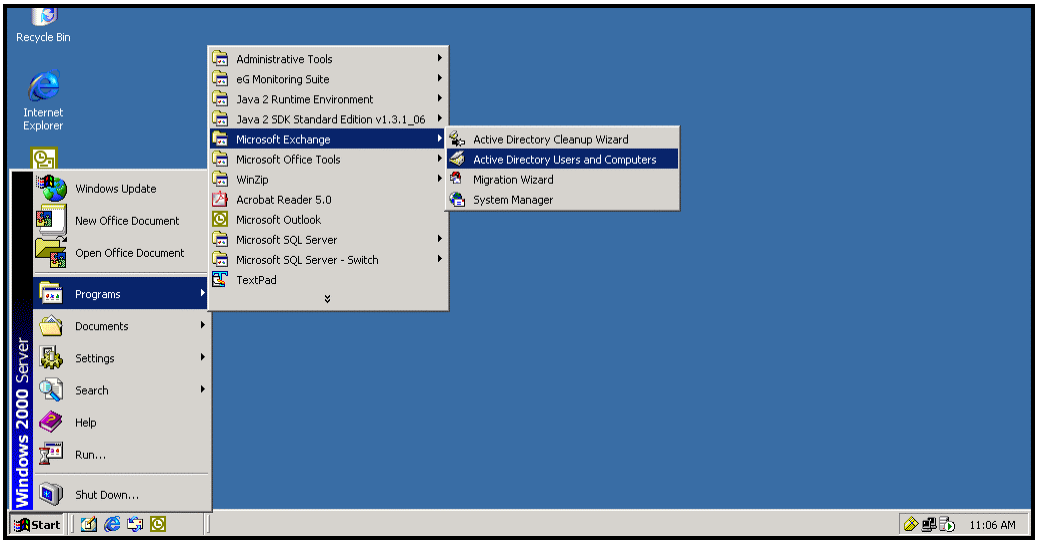

Figure 3.1: Opening the Microsoft Exchange Active Directory Users and Computers window

b. The window that appears has a tree structure in its left pane. Expanding the Active Directory Users and Computers node in the left pane will reveal a list of sites on the Exchange server. Expand the site on which the new mailbox is to be created, right-click on the **Users** folder within, select **New** from the shortcut menu that appears, and choose the **User** option from the **New** menu (see Figure 3.2).

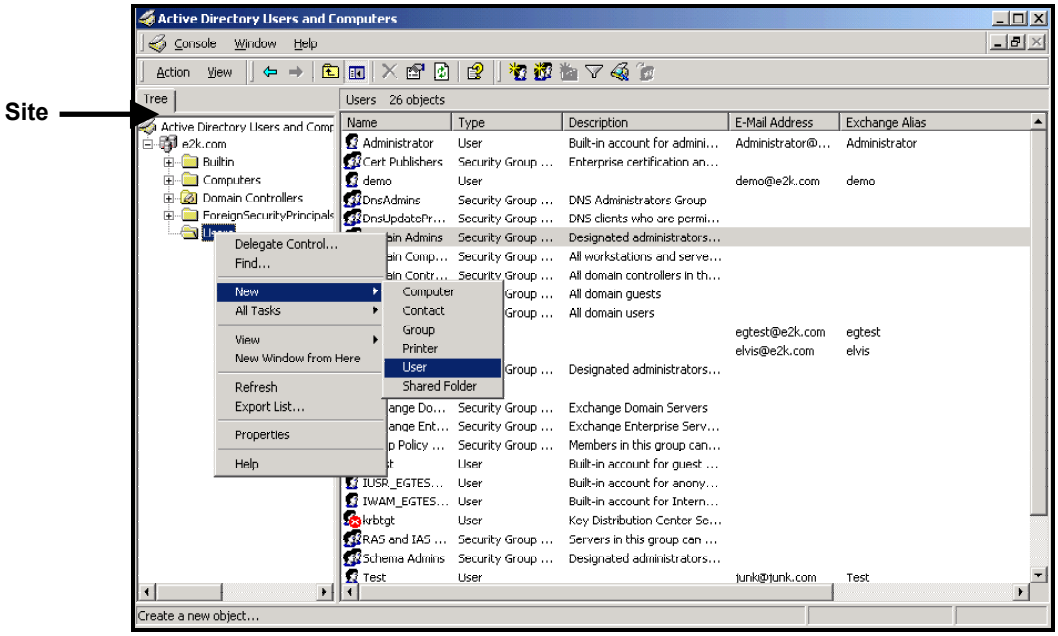

Figure 3.2: Creating a new Exchange mail box for user *john*

c. In the **New Object – User** dialog box that appears (see Figure 3.3), specify the details of the mailbox being created. After providing the user name, specify a **User logon name** (the name using which the user logs into the Exchange server), and select the site on which the mailbox is being created from the adjoining list box (here, the site name will be prefixed by an '@' symbol) (see Figure 3.3). The **User logon name** and the **Site** name together forms the **Email ID** of the user mailbox. For example, in Figure 3.3 below, the **Email ID** of the **mailbox** *elvis* is *elvis@e2k.*com. This is the email ID that will have to be specified against the **XCHGMAILBOXNAME** parameter.

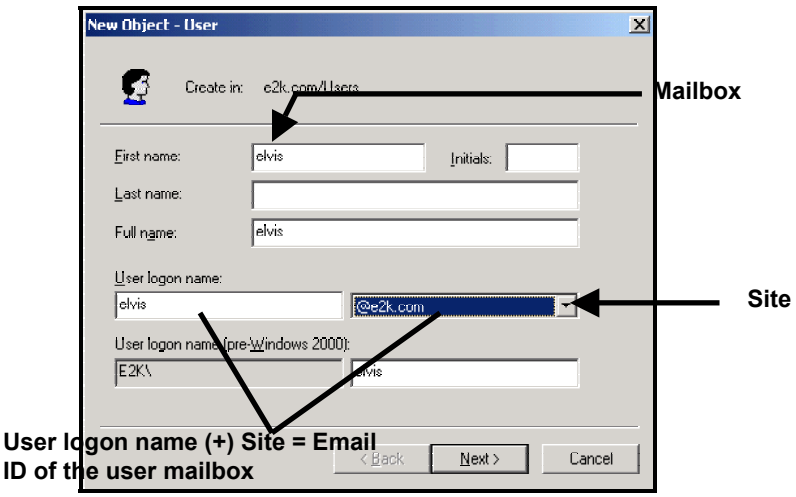

Figure 3.3: Specifying the details of the new user account

d. Next, specify the **Password** for the new user account and confirm it by retyping it in the **Confirm Password** text box. Then, check the **Password never expires** check box and click the **Next >** button to continue (see Figure 3.4).

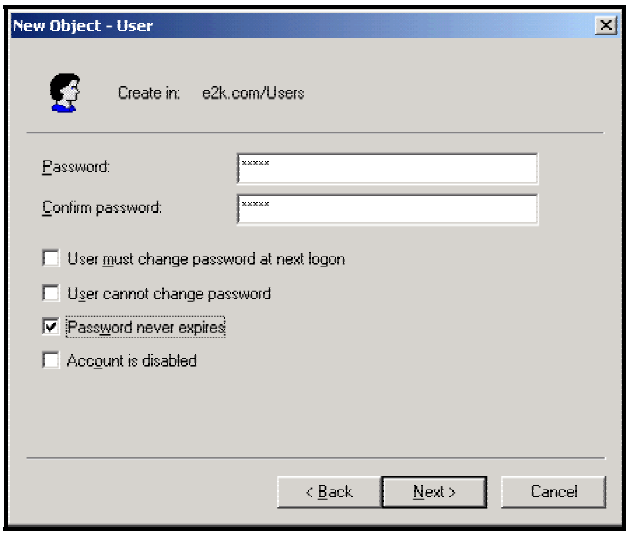

Figure 3.4: Specifying the password

e. Then, click on the **Create an Exchange mailbox** check box (see Figure 3.5) to create a mailbox for the user. Next, provide an alternate name for the mailbox

in the **Alias** text box, and then specify the full path to the **Server** which hosts the Exchange 2000 server (You can view the full path using the tree structure in the **System Manager** window that appears when the following menu sequence is followed: Start -> Programs -> Microsoft Exchange -> System Manager). Also, specify the **Mailbox Store** and click the **Next >** button to continue.

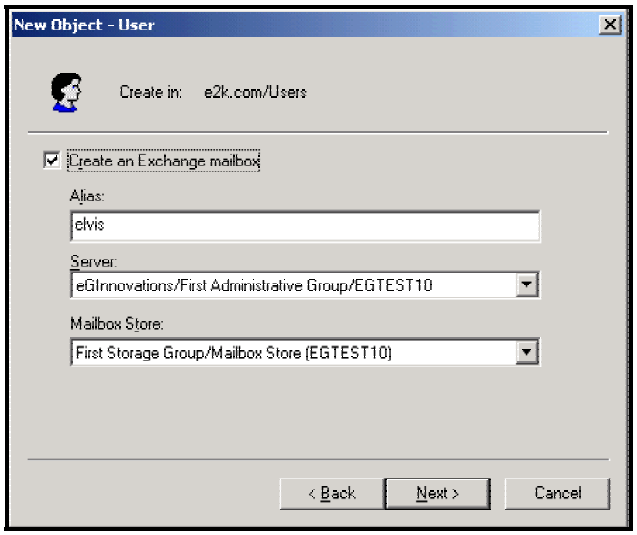

Figure 3.5: Creating a mailbox

f. Finally, view a summary of your specifications, and click the **Finish** button to quit setup (see Figure 3.6).

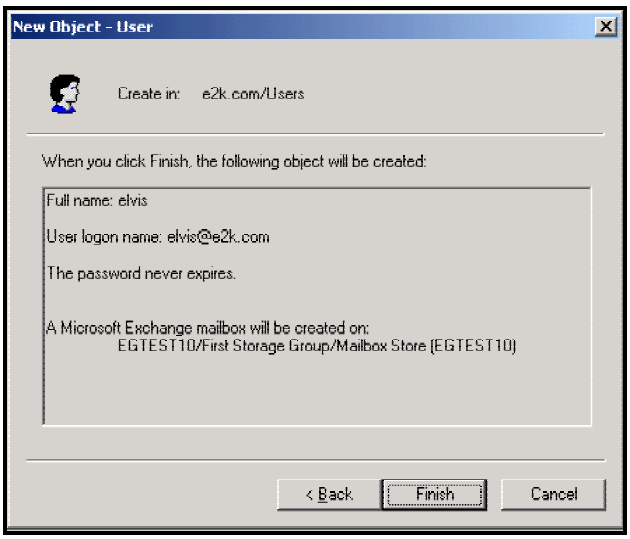
New Object - User
Create in: e2k.com/Users
When you click Finish, the following object will be created:
Full name: elvis
User logon name: elvis@e2k.com
The password never expires.
A Microsoft Exchange mailbox will be created on:
EGTEST10/First Storage Group/Mailbox Store (EGTEST10)
< Back
Finish
Cancel

Figure 3.6: Summary of the specifications

g. The eGurkhaAgent service should run using the account information of the user whose mailbox has been configured for the XChgMail test.

h. By default, the eGurkhaAgent service uses the LocalSystem account for execution. This account however, may not permit an external agent to access the mailbox that has been configured for the XChgMailTest. Hence, the

eGurkhaAgent service should be made to run using the login information of the user whose mailbox has been configured for the XChgMail test.

i. For example, assume that the administrator has decided to use the Windows 2000 user *elvis's* mail box for configuring the XChgMail test. To login to a Windows 2000 server/client, *elvis* uses the user name *elvis* and the password *elvis*. To ensure that the external agent gains access to *elvis's* mailbox for monitoring, the above-mentioned login information should be passed to the eGurkhaAgent service. The process to be followed for performing this, has already been discussed.

j. MAPI should be configured in the Exchange 2000/2003 server.

k. MAPI is used by an Exchange server (5.5/2000/2003) for internal messaging purposes. The XChgMail test and the MsXMail test require MAPI to be up and running in the Exchange server. While this service is configured in an Exchange server 5.5 by default, it is not the case in an Exchange 2000/2003 server. To configure this service, do the following:

   i. Open the **Active Directory Users and Computers** window using the menu sequence: Start -> Programs -> Microsoft Exchange -> Active Directory Users and Computers.

   ii. In the tree-structure in the left pane, expand the node representing the site on which a mail box for the eG user has been configured. Click on the **Users** folder within the site, so that the complete list of mailboxes appears in the right pane. Now, double-click on the eG user's mailbox. Then, click on the **E-mail Addresses** tab (see Figure 3.7) of the **Properties** dialog box that appears:

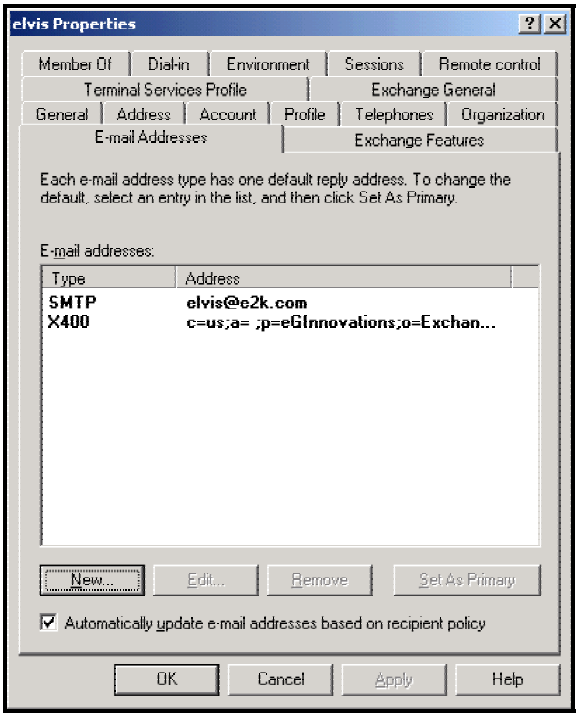

Figure 3.7: The E-mail Addresses tab

iii. To add the MAPI email-address to the list of addresses displayed

therein, click on the **New** button in Figure 3.7. Upon clicking, an **E-mail address type** list will appear (see Figure 3.8). Select **Microsoft Mail Address** from that list and click the **OK** button (see Figure 3.8).

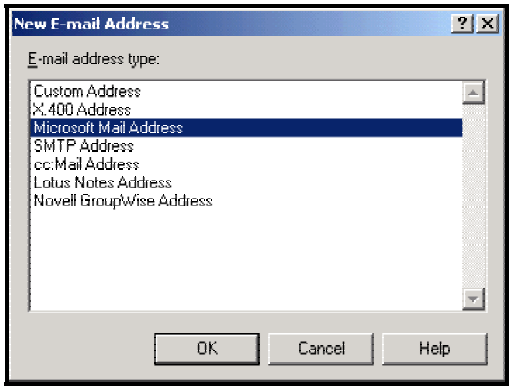

Figure 3.8: Selecting Microsoft Mail Address as the address type

iv. In Figure 3.8 that appears next, specify the properties of the chosen address type. Enter the name of the organizational unit (see Figure 3.9) that houses the mailbox, in the **Network name** text box. Then, in the **Postoffice name** text box, specify the name of the site (see Figure 3.9) on which the mailbox has been configured. Finally, the **Mailbox name** (see Figure 3.9) is to be specified.

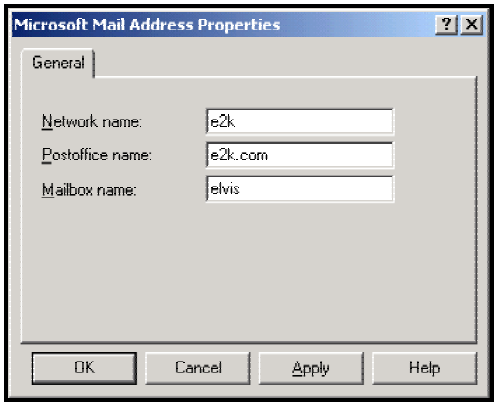

Figure 3.9: Specifying the properties of the address type

v. Next, click on the **Apply** button, and then the **OK** button to return to Figure 3.9. Finally, click on the **Apply** and **OK** buttons in Figure 3.7 to complete the process of creating the MAPI service.

3.2 Administering the eG Manager to monitor an Exchange 2000/2003 Server

After installation of the eG agent, follow the following steps to configure eG to monitor Exchange 2000/2003 servers.

1. Login to eG user interface as an administrative user.
2. If the Exchange Server 2000/2003 (referred to as *Exchange* in the eG Enterprise system) is already discovered, use the menu sequence Infrastructure -> Components -> Manage/Unmanage to manage it. The screens below depict the process of managing an Exchange 2000/2003 server clearly.

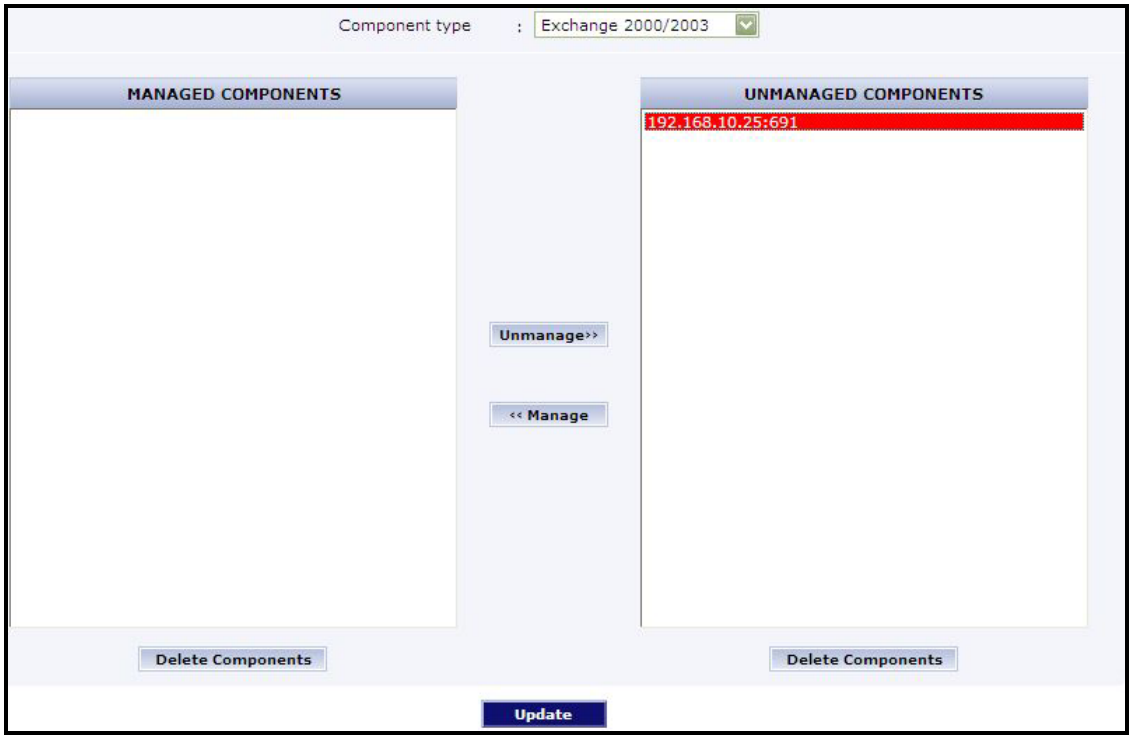

Figure 3.10: Viewing the list of unmanaged Exchange 2000/2003 servers

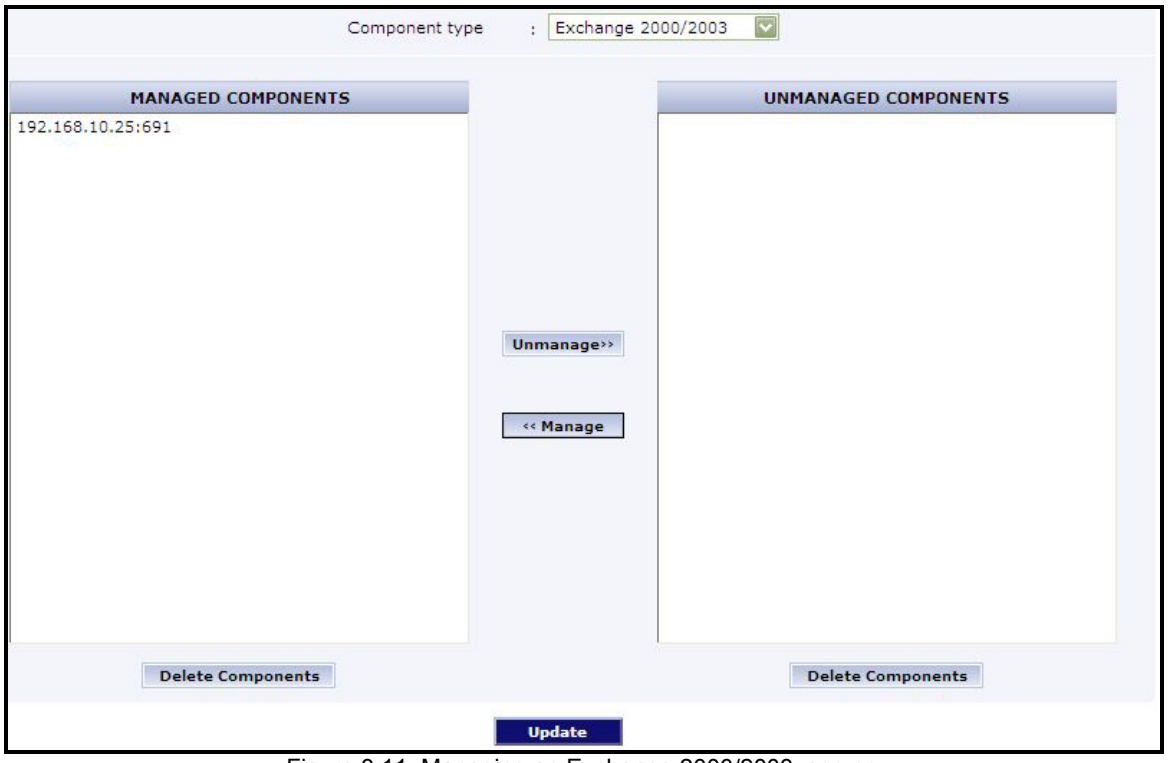

Figure 3.11: Managing an Exchange 2000/2003 server

3. On the other hand, if the component is not discovered, run discovery to get the Exchange 2000/2003 servers discovered or manually add them. Proceed to manage discovered components as discussed above. Components manually added, are however, automatically managed.

Refer

Please refer to Configuring and Monitoring Web Servers document for a more elaborate discussion on how to discover components, add them manually and manage them.

4. Once again, on signing out, you would be prompted to configure the tests depicted by Figure 3.12.

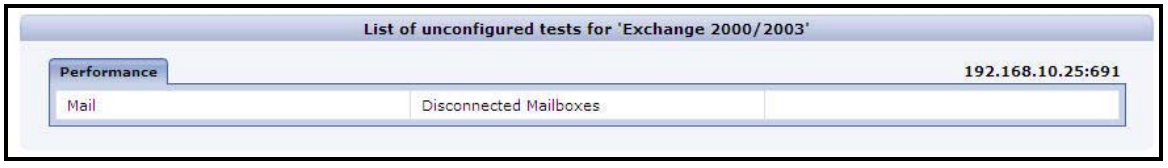

Figure 3.12: The list of unconfigured tests for an Exchange 2000/2003 server

5. If the Exchange Mail test is already configured (for eg., while configuring a Exchange server), then no such prompt will appear. Figure 3.13 displays the parameters of the Mail test for an Exchange 2000/2003 server.

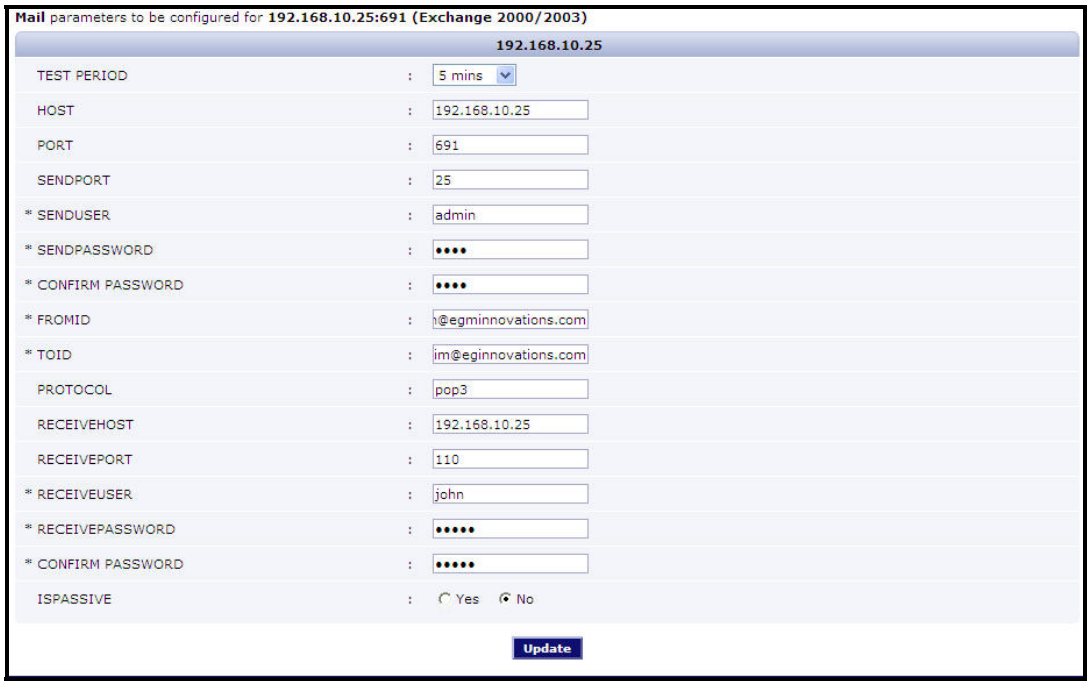

Figure 3.13: Mail test for an Exchange 2000/2003 server

6. Note that the Mail test for an Exchange 2000/2003 server consists of an additional **ISPASSIVE** parameter. This parameter will be available for every Exchange 2000/2003 test uptill the **Application Processes** layer. If the value chosen against this parameter is **YES**, then the Exchange 2000/2003 server under consideration is a passive server in an Exchange cluster. No alerts will be generated if the server is not running. Measures will be reported as "Not applicable' by the agent if the server is not up.
7. If you try to sign out again, you will be prompted to configure the Disconnected Mailboxes test. This test automatically discovers and monitors the disconnected mailboxes on an Exchange server. The parameters of the test are depicted by Figure 3.14.

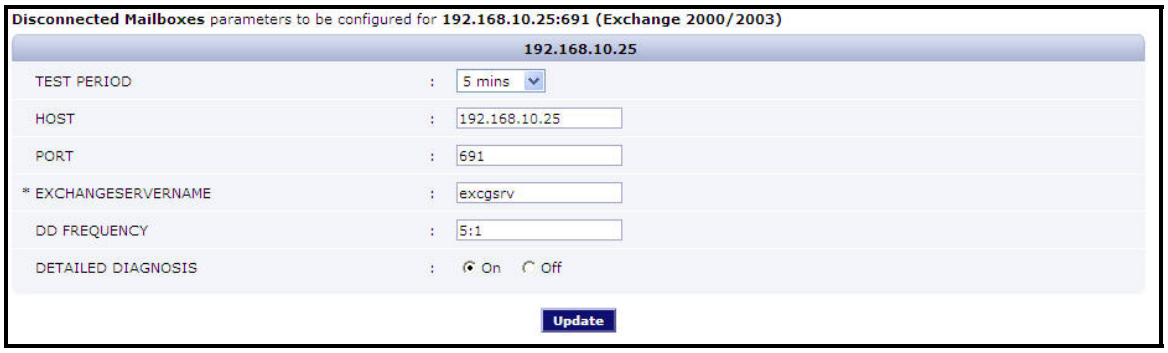
Disconnected Mailboxes parameters to be configured for 192.168.10.25:691 (Exchange 2000/2003)
192.168.10.25
TEST PERIOD : 5 mins
HOST : 192.168.10.25
PORT : 691
* EXCHANGESERVERNAME : excgsrv
DD FREQUENCY : 5:1
DETAILED DIAGNOSIS : On Off
Update

Figure 3.14: Configuring the Disconnected Mailboxes test

8. In Figure 3.14, specify the following:
   - **TEST PERIOD** - How often should the test be executed
   - **HOST** - The IP address of the machine where the Exchange Server is installed.
   - **PORT** – The port number through which the Exchange Server communicates.

- **EXCHANGESERVERNAME** - Enter the name of the Exchange server to be monitored.
- **DD FREQUENCY** - The **DD FREQuENCY** refers to the frequency with which detailed diagnosis measures are to be generated. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. Typically, detailed diagnosis frequencies are set globally, using the **DIAGNOSIS CONFIGURATION** page that appears when the Configure -> Diagnosis menu sequence is followed. This global setting can be overridden at the test-level using the **DD FREQUENCY** parameter. To disable the detailed diagnosis capability for a test, you can set this parameter to 0:0.
- **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

  The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

  - The eG manager license should allow the detailed diagnosis capability
  - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

9. Finally, click the **Update** button.

The Mapi Mail Service test emulates a client connecting to an Exchange 2000/2003 server and sending/receiving mails. The eG Enterprise system, by default, switches off the execution of the XchgMail test. An administrator can optionally turn this test on, so that it can be executed on the Exchange 2000/2003 server.

Figure 3.15 depicts the complete list of performance tests that are enabled and disabled by default for the chosen Exchange 2000/2003 component type. To enable the test open the **ENABLE-DISABLE TESTS** page by following the menu sequence *Agents -> Tests -> Enable/Disable*. In this page, you can either preclude or exclude a test from being executed for a specific a test type of a component type.

For an example, to preclude any of the performance tests of exchange 2000/2003 component type, select the desired options from the drop-down list as depicted by the figure. Now select the test names from the **DISABLED TESTS** list box and click on the button. (see Figure 3.15).

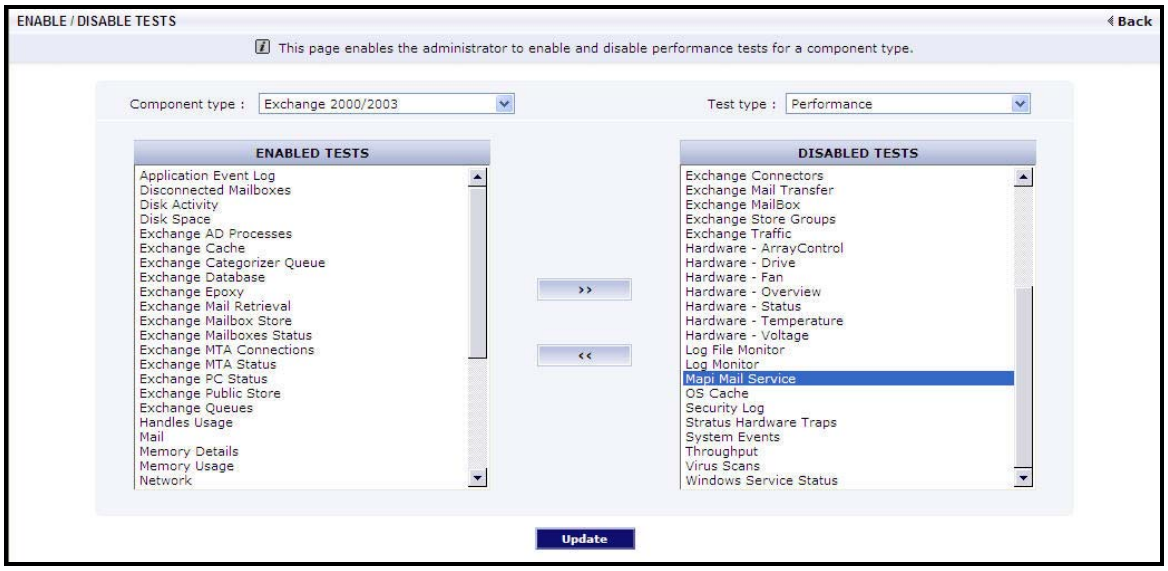

Figure 3.15: Selecting the tests to be enabled for Exchange 2000/2003 server

Figure 3.16 depicts the chosen tests of Exchange 2000/2003 component type have been precluded in the **ENABLED TESTS** list box. Click on **Update** button to implement the changes.

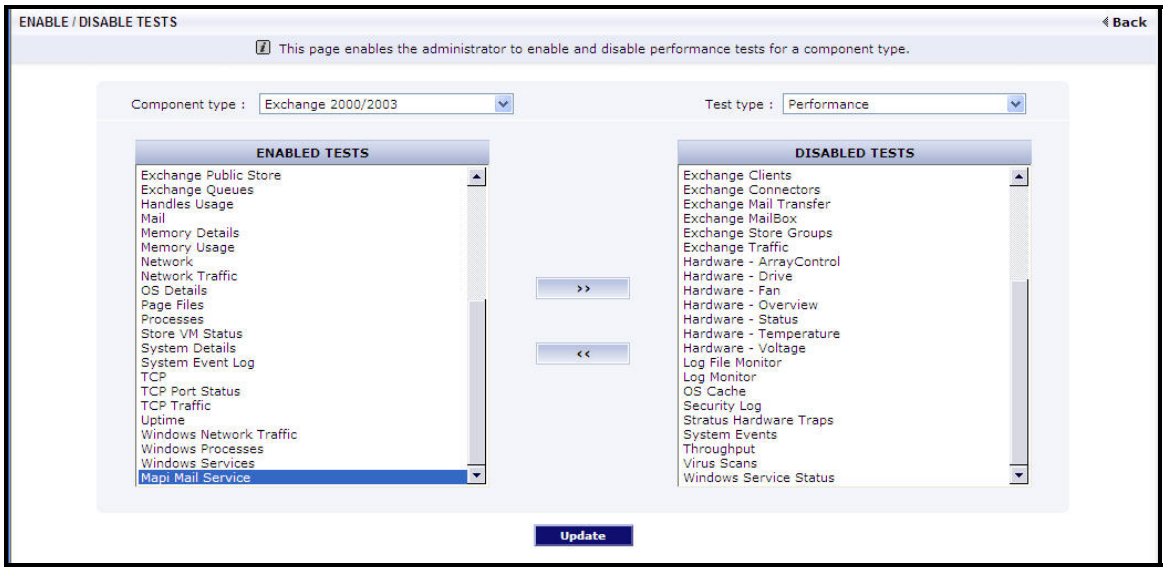

Figure 3.16: Enabling the tests for the Exchange 2000/2003 server

10. Then, return to the **AGENTS – TESTS SPECIFIC CONFIGURATION** page using the menu sequence **Agents** -> **Tests** -> **Configure** -> **Specific**.

    First choose Exchange 2000/2003 from the **Component type** list box and the specific component from the **Component name** list box. Then choose type of a test say as Performance from the **Test type** list box. Doing so will provide the agent summary details

and as well the configuration status of all the tests pertaining to the chosen component respectively.

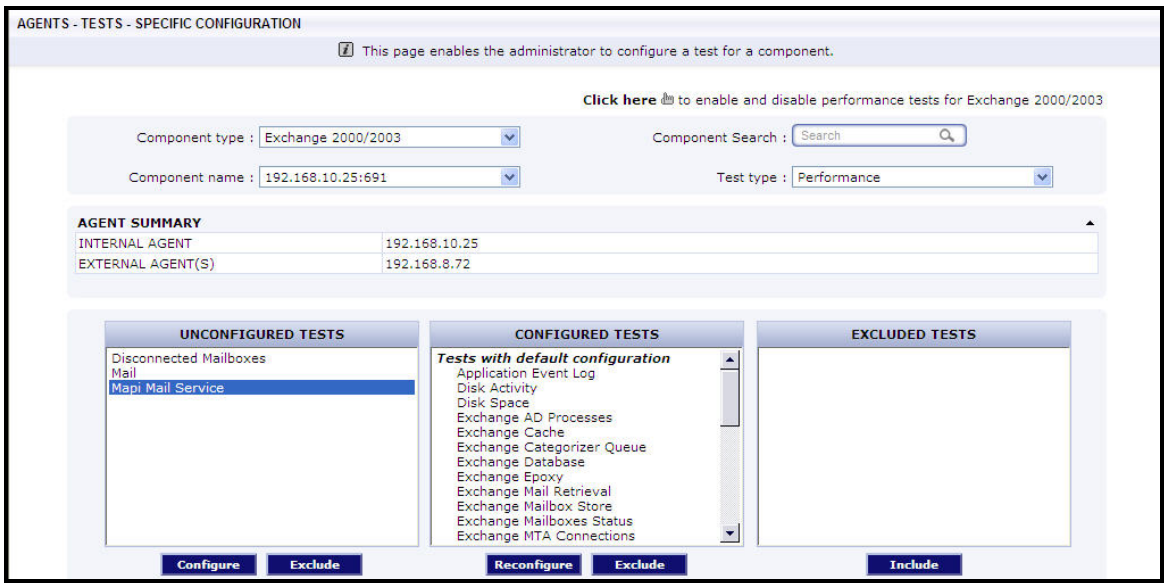

Figure 3.17:Selecting Mapi Mail Service test from the unconfigured tests

To configure an unconfigured test, select the MapiMailService test from the **UNCONFIGURED TESTS** list box and click on the **Configure** button. This will invoke the parameters to be configured for the chosen test. Finally click on the **Update** button to implement the changes as depicted by the Figure 3.17.

11. Upon clicking, the test parameters will be displayed:

- **TEST PERIOD** - How often should the test be executed
- **HOST** - The IP address of the machine where the Exchange 2000/2003 server is installed.
- **PORT** – The port number through which the Exchange 2000/2003 server communicates. The default port number is 691.
- **ISPASSIVE** - If the value chosen is **YES**, then the Exchange 2000/2003 server under consideration is a passive server in an Exchange cluster. No alerts will be generated if the server is not running. Measures will be reported as "Not applicable' by the agent if the server is not up. This parameter will be available for every Exchange server test uptill the **APP_PROCESSES** layer.
- **XCHGMAILBOXNAME** - Specify the email ID on the Exchange server that is to be used by this test for sending/receiving mails. To know the email ID that corresponds to a user mailbox, do the following:

    i. On the Exchange server, follow the menu sequence, Programs -> Administrative Tools (or Control Panel -> Administrative Tools) -> Active Directory Users and Computers.

    ii. Figure 3.18 will then appear. In the tree structure in the left pane of Figure 3.18, expand the node that corresponds to the **Site** on the Exchange server, and then, click on the **Users** folder within.

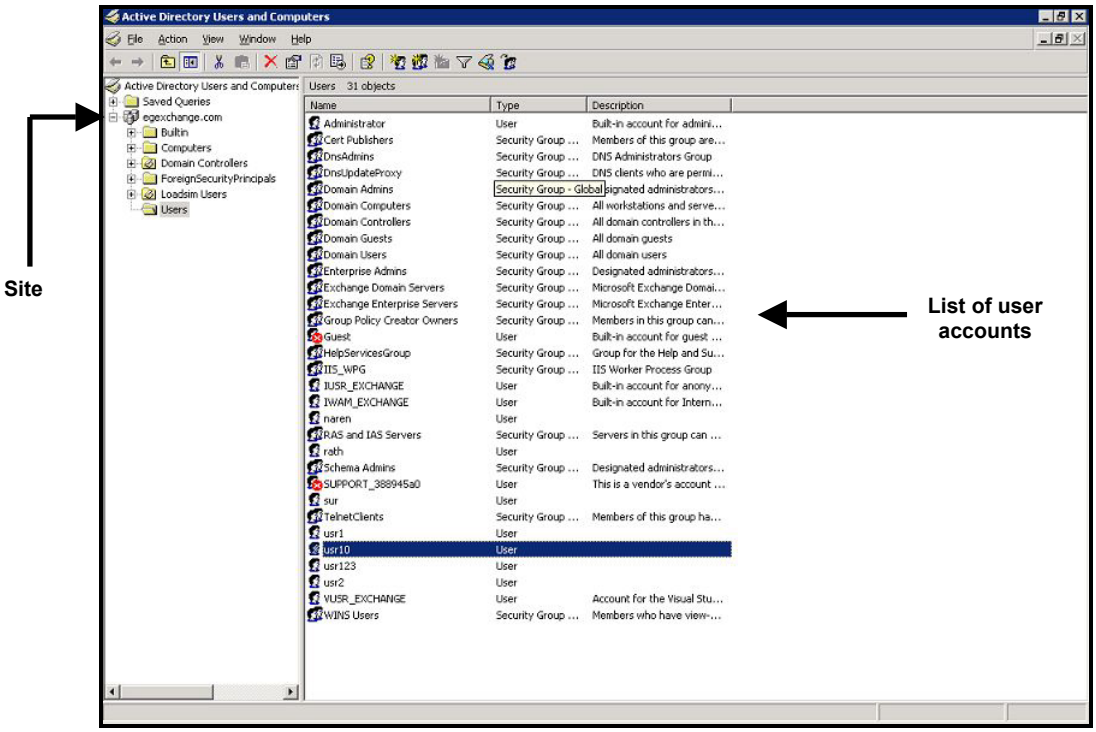

Figure 3.18: The Active Directory Users and Computers console

iii. From the list of user accounts displayed in the right pane, select the account that you intend using for the test and double-click on it.

iv. Figure 3.19 will then appear displaying the properties of the chosen mailbox. For configuring the **XCHGMAILBOXNAME** parameter of this test, specify the **E-mail** address displayed in Figure 3.19.

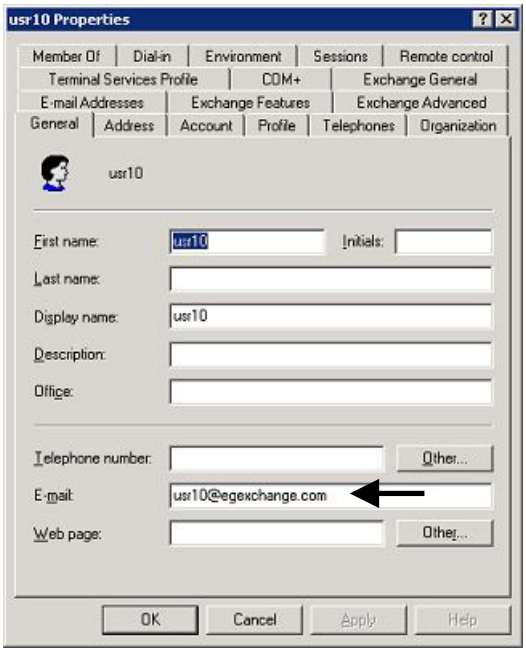

Figure 3.19: Properties of the chosen user account

a. **SMTPSERVER** - The IP address of the Exchange server being monitored; by default, the IP address of the **HOST** is displayed here.

b. **SMTPPORT** - The port number at which the **SMTPSERVER** listens; by default, it is 25.

c. **PROFILENAME** - The profile that the email ID in the **XCHGMAILBOXNAME** text box is configured to use. To know the existing profiles, open the **Control Panel** on the Microsoft Outlook 2003 client that houses the **XCHGMAILBOX** that has been configured for this test, and double-click on the **Mail** option within. The **Mail Setup** dialog box will open. Click on the **Show Profiles** button therein to view the existing list of profiles.

12. Finally, click the **Update** button.

13. Similarly, eG agents can also be configured to execute an Exchange MailBox test and an XchgStoreGroup test on the Exchange server. The XchgMailBox test automatically discovers all the mailboxes on a monitored Exchange 2000/2003 server, and reports the usage of each mailbox. The Exchange StoreGroupa test periodically observes the fluctuations in the store group size and the size of the mailbox and public folder stores within. These tests are also disabled by default. To enable the test open the **ENABLE-DISABLE TESTS** page by following the menu sequence *Agents -> Tests -> Enable/Disable*. In this page, you can either preclude or exclude a test from being executed for a specific a test type of a component type. select the test names from the **DISABLED TESTS** list box and click on the **<<** button. Click on **Update** button to implement the changes. Then, return to the **AGENTS – TESTS SPECIFIC CONFIGURATION** page using the menu sequence **Agents -> Tests -> Configure -> Specific**.

14. Next select appropriate options from the **Component type**, **Component name**, **Test type** list boxes. Doing so will provide the agent summary details and as well the configuration status of all the tests pertaining to the chosen component respectively.

    To configure an unconfigured test, select the Exchange MailBox test from the **UNCONFIGURED TESTS** list box and click on the **Configure** button. This will invoke the parameters to be configured for the chosen test. Finally click on the **Update** button to implement the changes.

15. Figure 3.20 depicts the following parameters:

- **TEST PERIOD** - How often should the test be executed
- **HOST** - The IP address of the machine where the Exchange server is installed.
- **PORT** – The port number through which the Exchange server communicates.
- **LOGONUSER** - By default, a "*" is displayed here, indicating that the test automatically discovers all the mailboxes configured for all the users on the Exchange server.
- **EXCHANGESERVERNAME** - The name of the Exchange server instance on which mailbox monitoring is to be performed.

Figure 3.20: Configuring the XchgMailBox test

Note:

In order to enable this test to run, the eG agent executing the test should be run using the Exchange administrator account.

16. Similary, you can configure the XchgStoreGroup test also.
17. Once you are done with the configuring, sign out of the administrative interface.
18. Then, start the eG agent on the system that is hosting the Exchange 2000/2003 server.

3.3 Monitoring the Exchange 2000/2003 Server

1. Login to the monitor user interface of an *Exchange 2000/2003* server.
2. Click on the **COMPONENTS** option in the menu bar, and select the **Servers** option from the **COMPONENTS** menu.
3. View the *Exchange 2000/2003* server in the independent components list and click on it to view the layer model, tests, and measurements of the Exchange server.

3.4 Troubleshooting

The XchgMail test mimics the mail client activity by using the MAPI (Messaging Application Programming Interface) for sending and receiving mails. If this test does not report measures, then it could indicate that the test is unable to send mails using the test parameters that have been configured. To verify this, run the following command from the command prompt of the Microsoft Outlook 2003 client on which the mailbox that has been configured for this test, exists:

cscript <Path_to_dir_containing_XChgMailTest.vbs>\XChgMailTest.vbs "<The profile name that has been configured for this test>" <Exchange mail box that has been used by this test> <SMTP Server IP configured for this test> <SMTP Port used by this test>

For example, assume that the XchgMailTest takes the following parameters:

XCHGMAILBOXNAME: egtester@egexchange.com

PROFILENAME: Outlook

SMTPSERVER: 192.168.10.228

SMTPPORT: 25

Also, assume that the **XChgMailTest.vbs** is available in the **C:\eGurkha\lib** directory.

In such a case, the command to execute the test will be as follows:

cscript c:\eGurkha\lib\XChgMailTest.vbs "Outlook" egtester@egexchange.com 192.168.10.28 25

If, upon execution, the command returns the measures of the XChgMailTest, it indicates that the test is functioning properly.

If the test does not execute properly, then either of the following may occur:

a) You might receive the following error message:

[C:\eGurkha\lib\XChgMailTest.vbs(66, 1) Collaboration Data Objects: The Microsoft Exchange Server computer is not available. Either there are network problems or the Microsoft Exchange Server computer is down for maintenance. [Microsoft Exchange Server Information Store - [MAPI_E_FAILONEPROVIDER(8004011D)]],]]

b) The message box depicted by Figure 3.21 may appear:

Microsoft Outlook
A program is trying to automatically send e-mail on your behalf.
Do you want to allow this?
If this is unexpected, it may be a virus and you should choose "No".
Yes
No
Help

Figure 3.21: Message box indicating a problem in sending mails

If the message (a) or any other message bearing references to *Collaboration Data Objects (CDO)* appears, then it indicates that the **Collaboration Data Objects** option was not enabled while installing the Microsoft Outlook 2003 client on the box. The Collaboration Data Objects (CDO) library allows you to access the Global Address List and other server objects, in addition to the contents of mailboxes and public folders. As the XChgMailTest actively uses this library, the absence of CDO results in the failure of the test. In such a case, follow the procedure given below to modify your installation, so that CDO is enabled:

1. Insert the **Microsoft Office** CD in your CD drive, and run its **Setup.exe** on the system hosting the Microsoft Outlook Client that has been configured for the XChgMailTest.
2. Figure 3.22 appears requesting your confirmation to reinstall/uninstall/add or remove features to your existing Microsoft Outlook installation.
3. Choose the **Add/Remove Features** option and click the **Next** button to proceed.

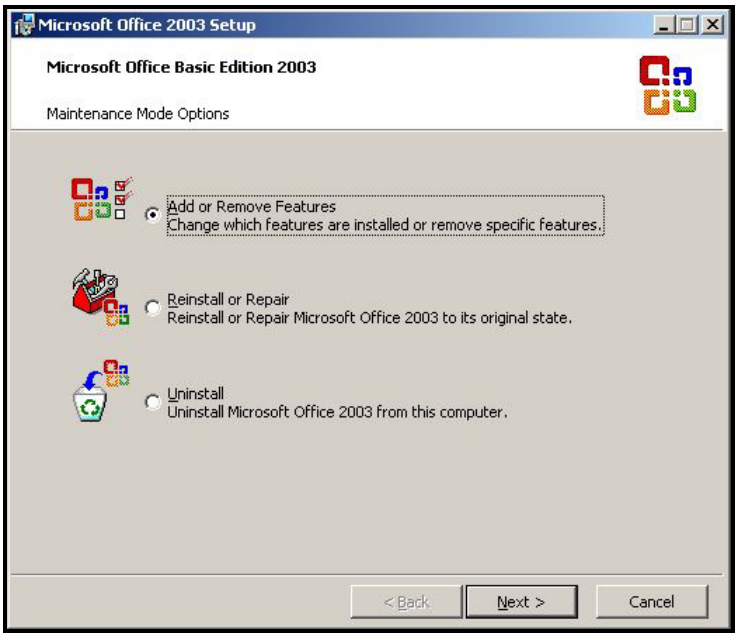
Microsoft Office 2003 Setup
Microsoft Office Basic Edition 2003
Maintenance Mode Options
Add or Remove Features
Change which features are installed or remove specific features.
Reinstall or Repair
Reinstall or Repair Microsoft Office 2003 to its original state.
Uninstall
Uninstall Microsoft Office 2003 from this computer.
< Back
Next >
Cancel

Figure 3.22: Selecting the 'Add/Remove Features' option

4. Then, select the **Outlook** option from Figure 3.23, and also click the **Choose advanced customization of applications** check box. Click the **Next** button to move on.

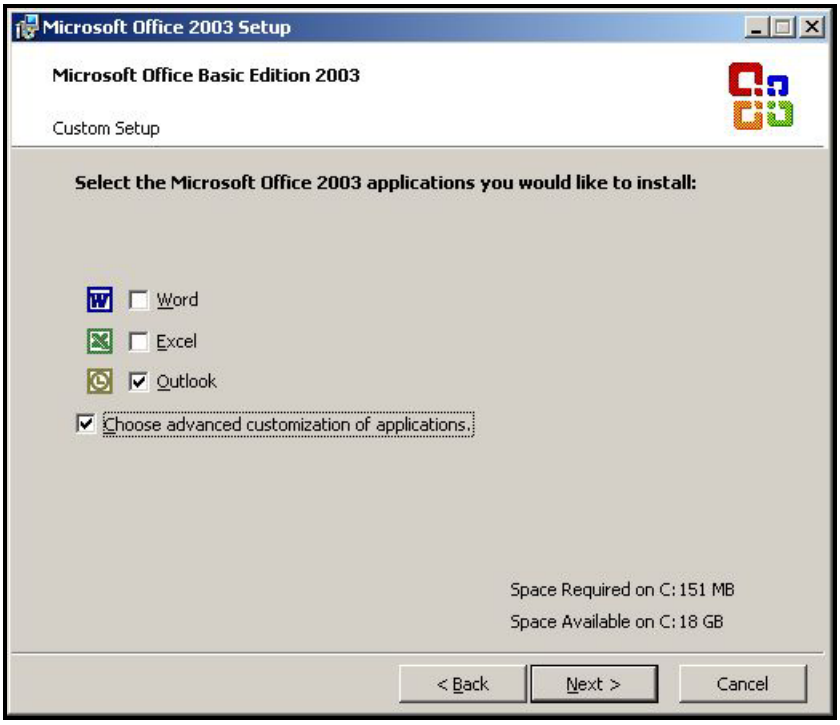

Figure 3.23: Choosing to customize the Outlook installation

5. In Figure 3.24 that appears next, expand the **Microsoft Office Outlook** tree to view the applications/tools within. By default, the **Collaboration Data Objects** option in the tree will be prefixed by an **X** mark, indicating that the option is disabled (see Figure 3.25). To enable

the option, click on the **X** mark, and select the **Run from My Computer** option from the shortcut menu that appears (see Figure 3.25).

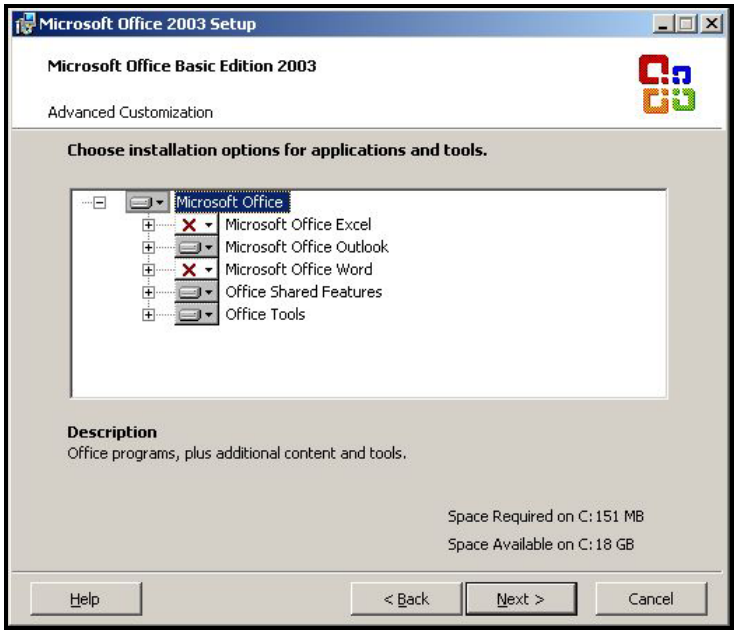

Figure 3.24: Viewing the currently installed applications

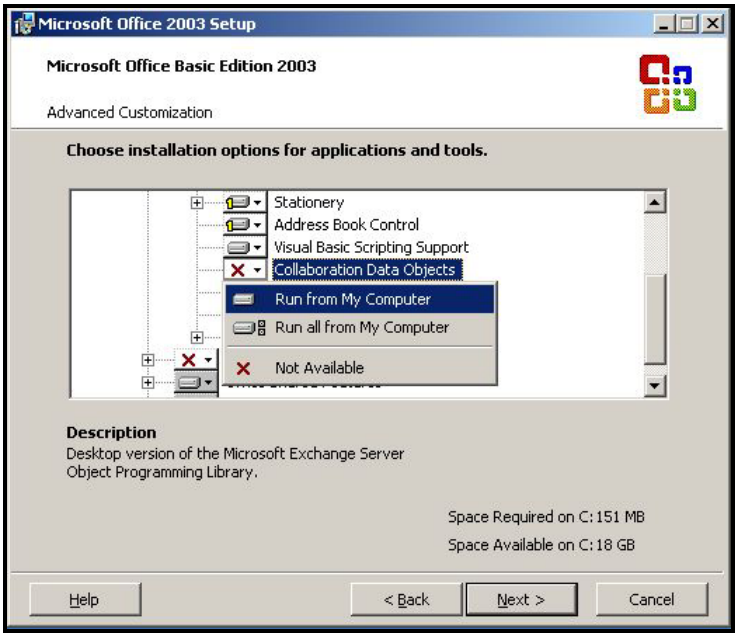

Figure 3.25: Selecting the Collaboration Data Objects option

6. Click on the **Next** button in Figure 3.25 to proceed.
7. Finally, when setup completes, click the **Finish** button to exit.

On the other hand, if manual command execution returned the message box depicted by Figure 3.21, it indicates that a security patch named **O2kSp3.exe** is installed on the Outlook client. To ensure that this patch does not affect the functioning of the XchgMail test, do the following:

8. Download **Orktools.exe** and **admpack.exe** from the following URL: http://www.microsoft.com/office/orkarchive/2000ddl.htm to the Outlook client.
9. Begin installing **Orktools.exe** on the Outlook client by double-clicking on it. Figure 3.26 will appear first.

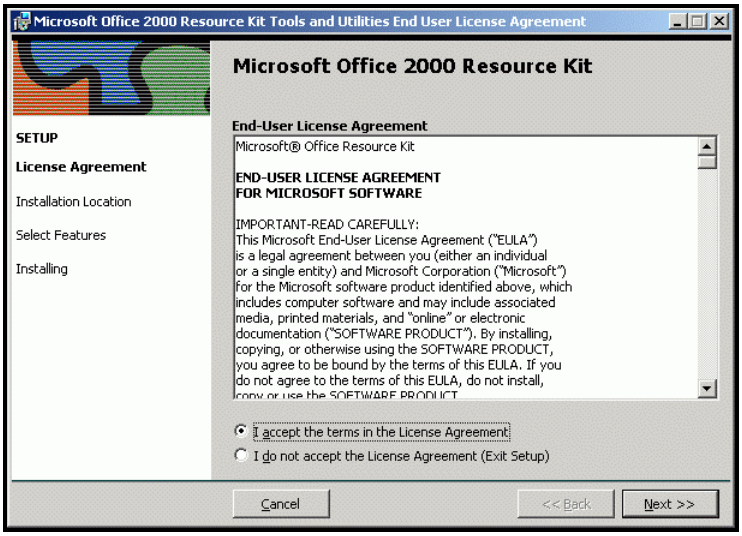
Microsoft Office 2000 Resource Kit Tools and Utilities End User License Agreement
Microsoft Office 2000 Resource Kit
SETUP
License Agreement
Installation Location
Select Features
Installing
End-User License Agreement
Microsoft® Office Resource Kit
END-USER LICENSE AGREEMENT
FOR MICROSOFT SOFTWARE
IMPORTANT-READ CAREFULLY:
This Microsoft End-User License Agreement ("EULA")
is a legal agreement between you (either an individual
or a single entity) and Microsoft Corporation ("Microsoft")
for the Microsoft software product identified above, which
includes computer software and may include associated
media, printed materials, and "online" or electronic
documentation ("SOFTWARE PRODUCT"). By installing,
copying, or otherwise using the SOFTWARE PRODUCT,
you agree to be bound by the terms of this EULA. If you
do not agree to the terms of this EULA, do not install,
I accept the terms in the License Agreement
I do not accept the License Agreement (Exit Setup)
Cancel
<< Back
Next >>

Figure 3.26: The End-use license agreement

10. Accept the license agreement displayed in Figure 3.26 by selecting the **I accept the terms in the License Agreement** option and clicking the **Next >>** button.
11. Figure 3.27 will then appear, from where an installation location will have to be selected. Then, click the **Next >>** button.

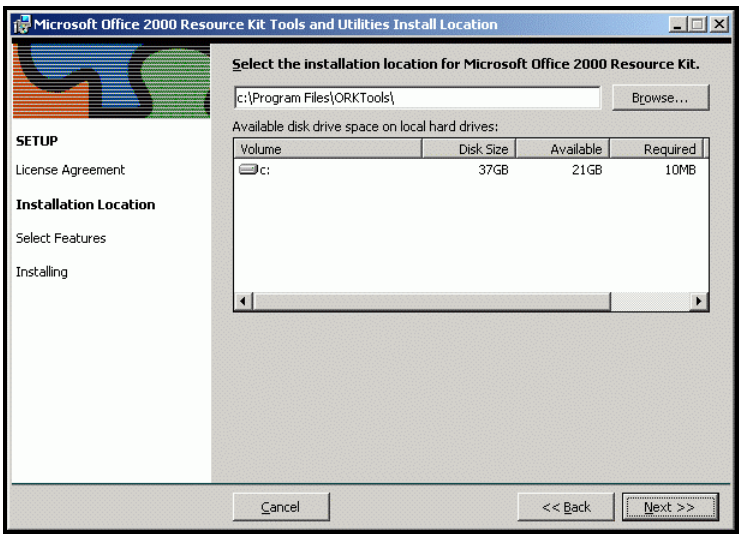

Figure 3.27: Selecting the install directory

12. Finally, click on the **Install Now** button in Figure 3.28 to begin installing the **Orktools.exe**.

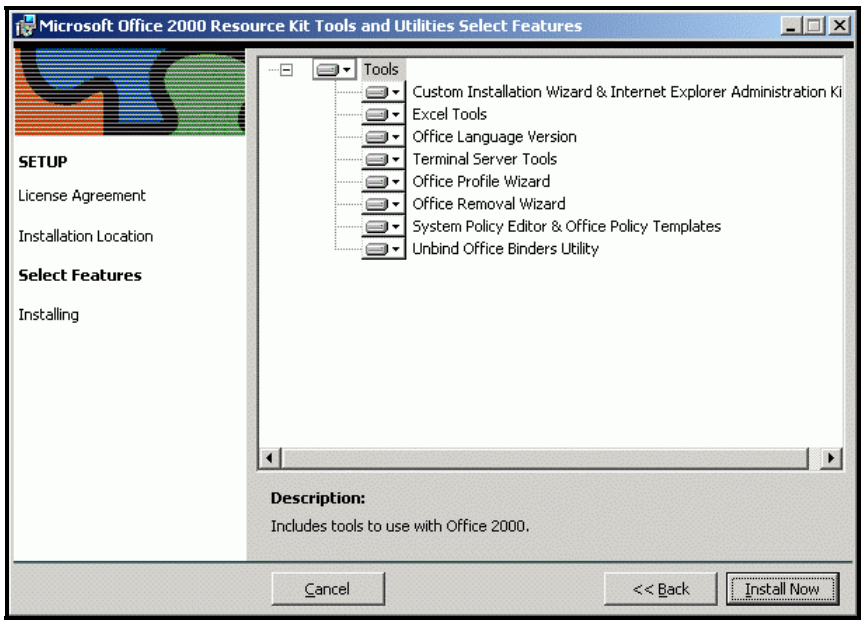

Figure 3.28: Installing Orktools.exe

13. Next, proceed to install **admpack.exe** on the Outlook client by double-clicking on it. Select **Yes** from Figure 3.29 that appears.

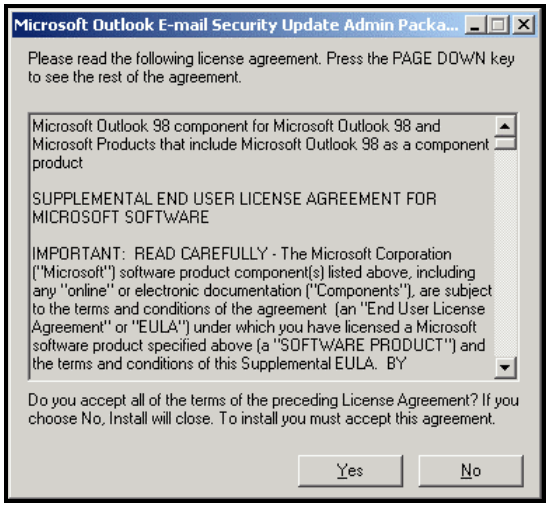
Microsoft Outlook E-mail Security Update Admin Packa...
Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.
Microsoft Outlook 98 component for Microsoft Outlook 98 and Microsoft Products that include Microsoft Outlook 98 as a component product
SUPPLEMENTAL END USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE
IMPORTANT: READ CAREFULLY - The Microsoft Corporation ("Microsoft") software product component(s) listed above, including any "online" or electronic documentation ("Components"), are subject to the terms and conditions of the agreement (an "End User License Agreement" or "EULA") under which you have licensed a Microsoft software product specified above (a "SOFTWARE PRODUCT") and the terms and conditions of this Supplemental EULA. BY
Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.
Yes
No

Figure 3.29: Accepting the license agreement for admpack.exe

14. Next, specify the location to which the files of **admpack.exe** need to be extracted, and then click the **OK** button (see Figure 3.30).

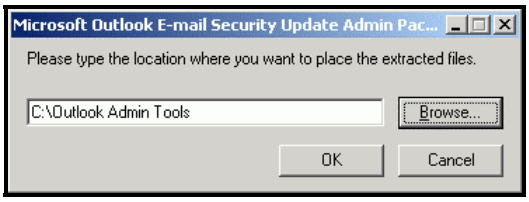
Microsoft Outlook E-mail Security Update Admin Pac...
Please type the location where you want to place the extracted files.
C:\Outlook Admin Tools
Browse...
OK
Cancel

Figure 3.30: Specifying the location of the admpack files

15. Once installation completes, Figure 3.31 will appear. Click on the **OK** button to exit the setup.

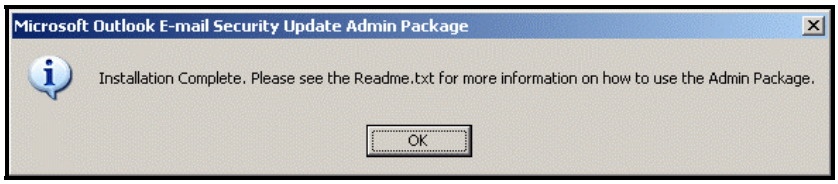
Microsoft Outlook E-mail Security Update Admin Package
Installation Complete. Please see the Readme.txt for more information on how to use the Admin Package.
OK

Figure 3.31: Completion of admpack installation

16. Then, go to the **Microsoft Exchange Server** and open its **System Manager** using the menu sequence depicted by Figure 3.32.

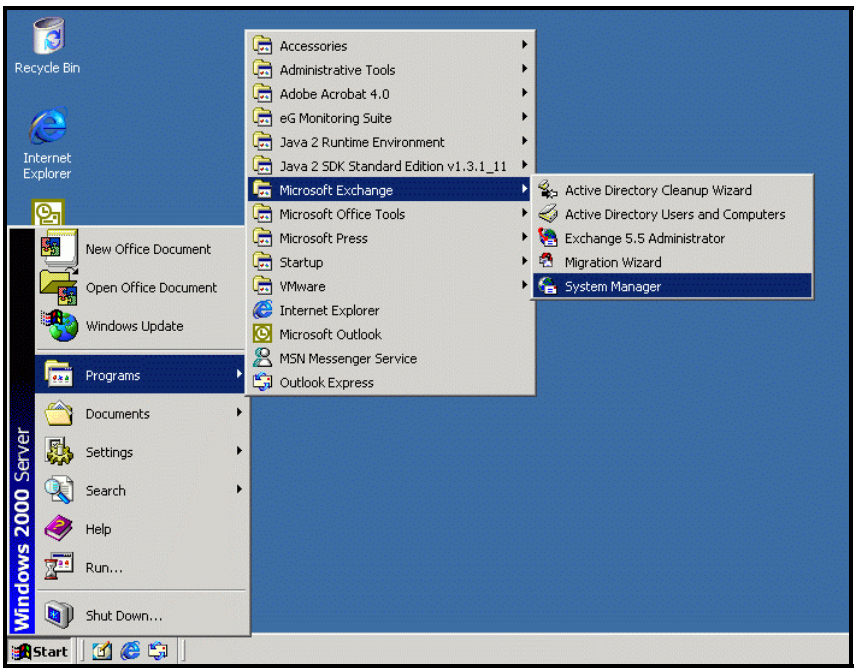

Figure 3.32: Opening the System Manager of the Microsoft Exchange Server 2000

17. Expand the **Folders** node in the tree-structure in the left pane of the System Manager, right-click on the **Public Folders** sub-node within, select the **New** sub-menu from the shortcut menu that appears, and then choose the **Public Folder** option, to create a new public folder on the Exchange server (see Figure 3.33).

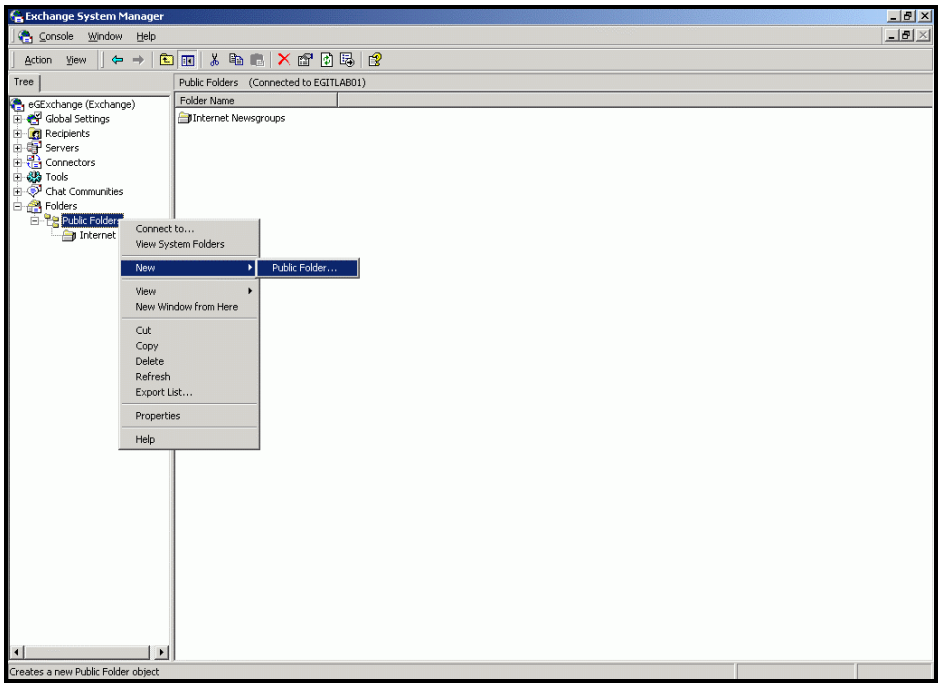

Figure 3.33: Creating a new Public Folder

18. Name the new public folder as **Outlook Security Settings** (see Figure 3.34), and then click the **Apply** and **OK** buttons therein to register the changes.

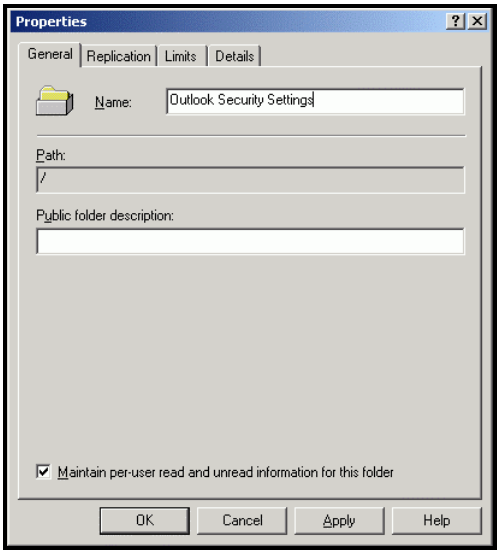

Figure 3.34: Naming the new public folder

19. Then, switch back to the Outlook client, and open the directory to which the files of **admpack.exe** have been extracted. Double-click on the **OutlookSecurity.oft** within to open the template file (see Figure 3.35).

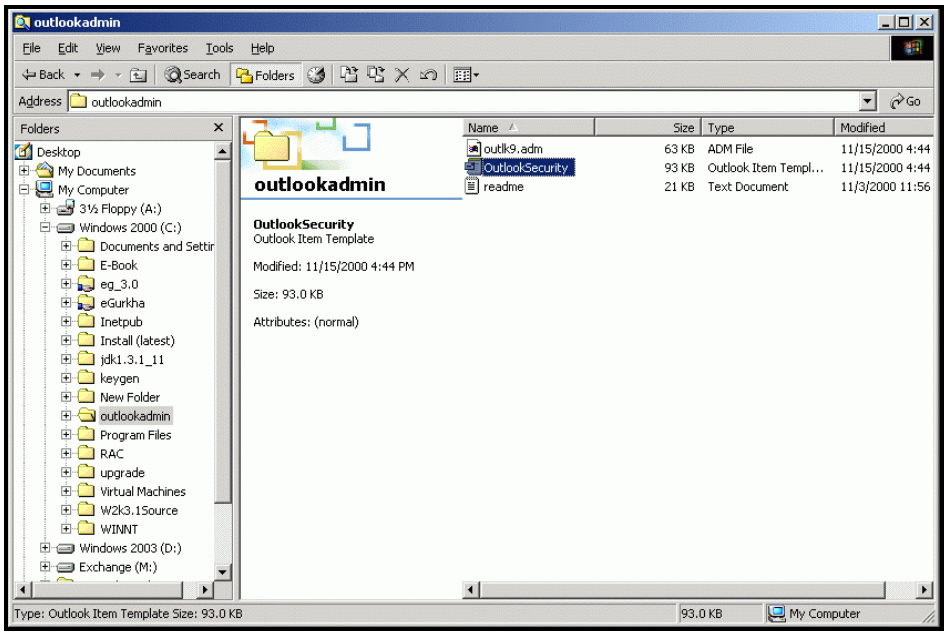

Figure 3.35: Opening the OutlookSecurity.oft template file

20. The **Select Folder** dialog box will then appear (see Figure 3.36). Expand the **Public Folders** node within, followed by the **All Public Folder** sub-node, and then select the **Outlook Security Settings** folder that was created in the Microsoft Exchange server. Next, click the **OK** button in Figure 3.36.

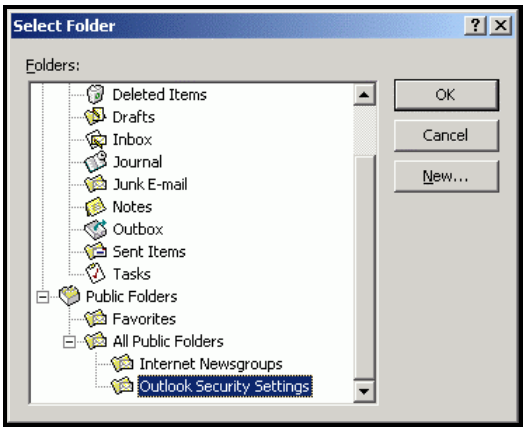

Figure 3.36: Selecting the Outlook Security Settings folder

21. The **Default Security Settings** form (see Figure 3.37) will open. Now, follow the menu sequence Tools -> Forms -> Publish Form (see Figure 3.37) to publish the form in the chosen **Outlook Security Settings** folder.

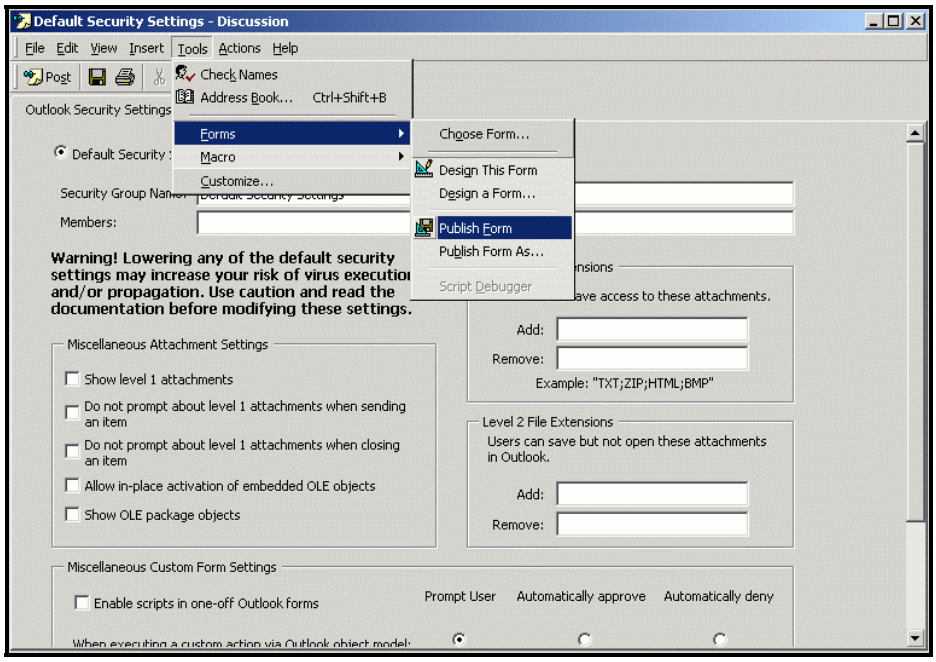
Default Security Settings - Discussion
File Edit View Insert Tools Actions Help
Post
Check Names
Address Book... Ctrl+Shift+B
Outlook Security Settings
Forms
Macro
Customize...
Choose Form...
Design This Form
Design a Form...
Publish Form
Publish Form As...
Script Debugger
Default Security
Security Group Name
Members:
Warning! Lowering any of the default security settings may increase your risk of virus execution and/or propagation. Use caution and read the documentation before modifying these settings.
Miscellaneous Attachment Settings
Show level 1 attachments
Do not prompt about level 1 attachments when sending an item
Do not prompt about level 1 attachments when closing an item
Allow in-place activation of embedded OLE objects
Show OLE package objects
Add:
Remove:
Example: "TXT;ZIP;HTML;BMP"
Level 2 File Extensions
Users can save but not open these attachments in Outlook.
Add:
Remove:
Miscellaneous Custom Form Settings
Enable scripts in one-off Outlook forms
Prompt User
Automatically approve
Automatically deny

Figure 3.37: Publishing the form

22. Provide the name **Outlook Security Form** to the form being published (see Figure 3.38), and click the **Publish** button to publish it.

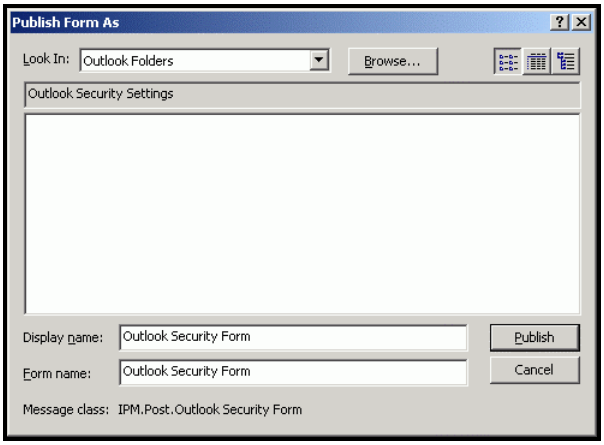

Figure 3.38: Specifying a name for the form

23. Close the form you opened from the .oft file.

24. Open **Microsoft Outlook**, select the **Outlook Security Settings** public folder, right-click on it, and choose **Properties** from its shortcut menu. In the **General** tab of the **Properties** dialog box that opens (see Figure 3.39), ensure that **Outlook Security Form** option is chosen from the **When posting to this folder, use** list box.

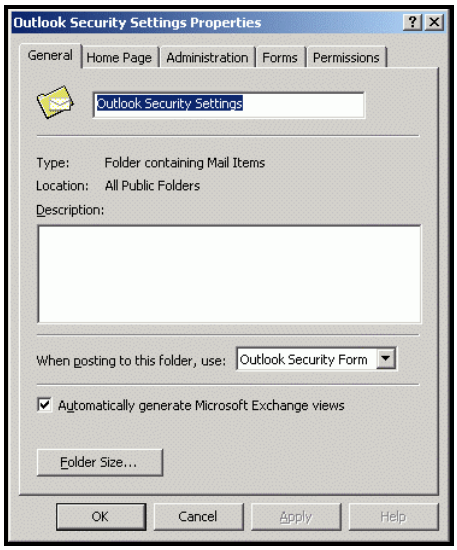

Figure 3.39: Choosing the Outlook Security Form option

25. Then, click on the **Permissions** tab in Figure 3.39, and set the **Reviewer** role for the **Default user** (see Figure 3.40). Give the Editor role only to people who administer Outlook security settings.

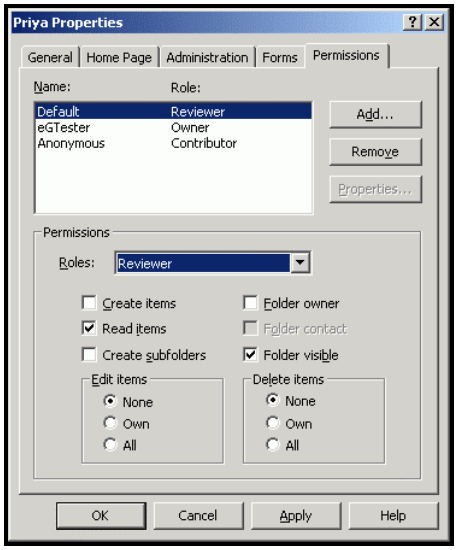

Figure 3.40: Selecting the Reviewer role

26. Finally, click the **Apply** button and then the **OK** button to save the changes.

Chapter 4

Configuring and Monitoring a Generic Mail Server

eG includes specialized models for Microsoft Exchange and Lotus Domino mail server. Any other mail server can be monitored as a generic mail server (referred to as *Mail* in the eG user interface). A generic mail server can be configured and monitored by following the steps given below:

- Administer the eG manager to monitor the generic mail server
- Monitor the Generic mail server

4.1 Administering the eG Manager to monitor a Generic Mail Server

1. Login to the administrative interface of eG as an administrator (admin).
2. Manually add the generic mail server to be monitored using the **ADD/MODIFY COMPONENTS** page (see Figure 4.1). To navigate to the **ADD/MODIFY COMPONENTS** page, follow the menu sequence: Infrastructure-> Components -> Add Modify.
3. The eG Enterprise system refers to Generic mail servers as *Mail*. To add a new generic mail server, first, select **Mail** as the **Component type** (as shown Figure 4.1 below) and then, click the **Add New Component** button.

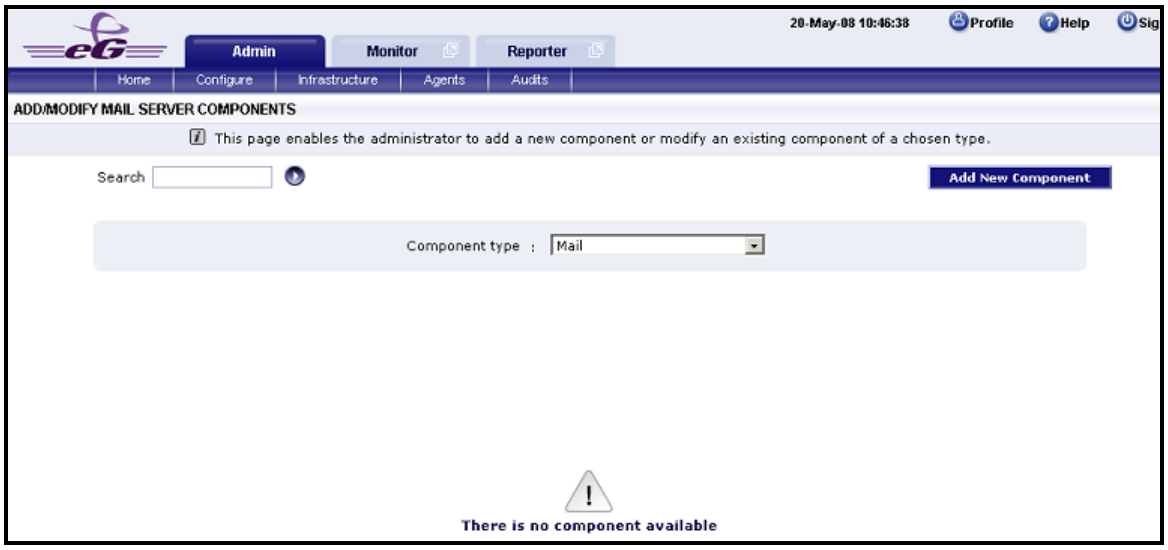

Figure 4.1: Selecting the type of component to be added

4. The following page will then appear. Specify the **Host IP** address of the new mail server, the **Host/Nick name** and the **Port number** at which the mail server listens to requests from clients. Then, click the **Add** button to register the changes.

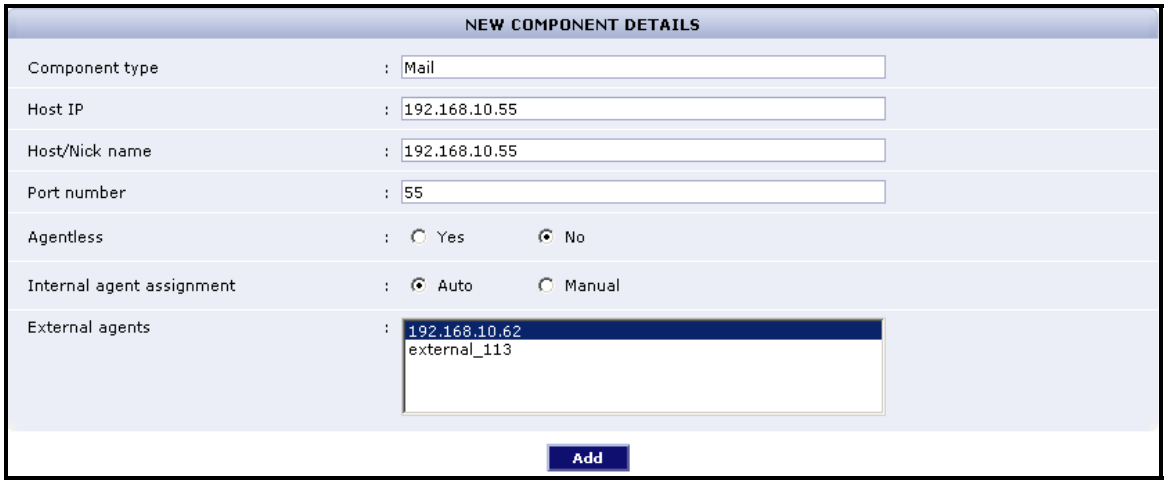

Figure 4.2: Adding the details of a new mail server

5. A summary of the new component details will then appear as shown in Figure 4.3 below.

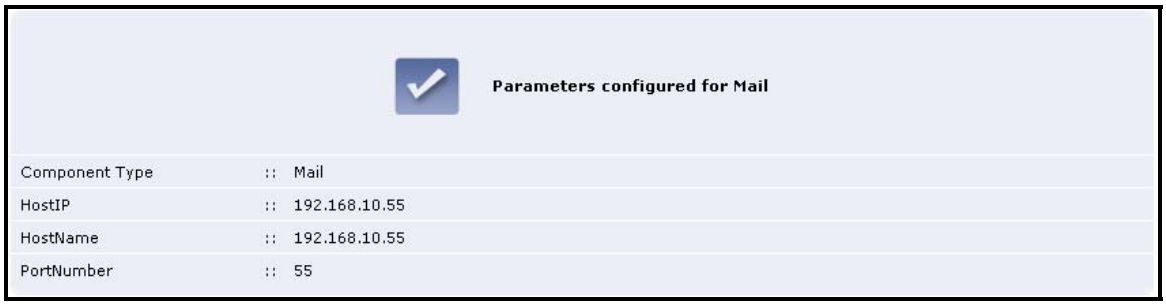

Figure 4.3: A page displaying a summary of the new mail server details

6. The Generic mail server so added will be managed automatically by eG Enterprise. Now, try to sign out of the user interface. Doing so, will bring up the following page, which prompts you to configure the Mail test and Processes test for the new Generic mail server.

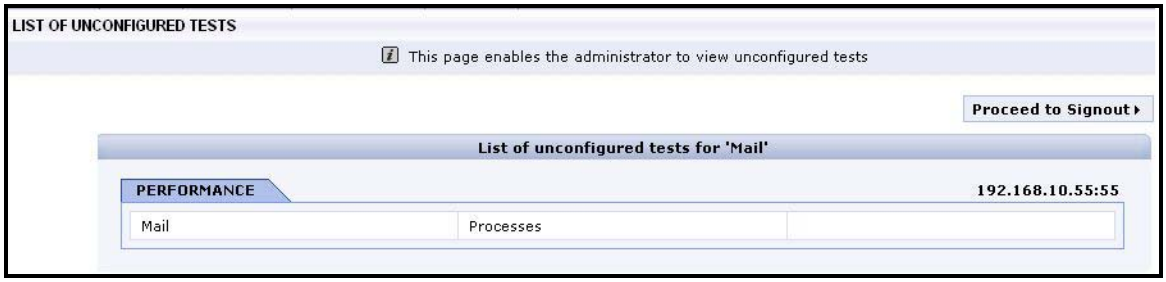

Figure 4.4: A page displaying the tests the need to be configured for the Generic mail server

7. Click on Mail test to configure it.

Refer Please refer to Section 1.3 above for a more elaborate discussion on how to configure the Mail test.

8. After configuring the Mail test, try to sign out once again.
9. You will now be prompted to configure the Processes test.

Refer Please refer to Configuring and Monitoring Web Servers document for a more elaborate discussion on how to configure the Processes test.

10. Once the Processes test parameters are configured, log out of the administrative interface.

4.2 Monitoring the Generic Mail Server

1. Login as a monitor / supermonitor user.
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. Click on the Generic *Mail* Server being monitored to view its measurements.

Chapter 5

Configuring and Monitoring a Qmail Server

This chapter describes the procedures involved in configuring and monitoring a Qmail server.

5.1 Configuring a Qmail Server to work with the eG Manager

For the Qmail tests to work effectively, ensure that the following are in place:

- The following packages (or their latest versions) should be installed along with Qmail:
  - netqmail-1.05
  - daemontools-0.76
  - ucspi-tcp-0.88

A detailed Qmail installation procedure is available in the following URL: /http://www.lifewithqmail.org/.

- All executable files (under **/package/admin/daemontools-0.76/command**) related to the qmail admin services should have links under **/usr/local/bin**.
- The executable file **svstat** (in the **/usr/local/bin** directory) must be given special executable permission using the command: **chmod u+s svstat**.
- The eG user should be added to the **qmail** group.

5.2 Administering the eG Manager to monitor a Qmail Server

To achieve this, do the following:

1. Login to the administrative interface of eG as an administrator (admin).
2. If a Qmail server is already discovered, then directly proceed towards managing it using the **MANAGE/UNMANAGE** page (Infrastructure -> Components -> Manage/Unmanage). However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or add the component manually using the **ADD/MODIFY COMPONENTS** page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are managed automatically. Discovered components,

however, are managed using the **MANAGE/UNMANAGE** page. Figure 5.1 and Figure 5.2 clearly illustrate the process of managing the Qmail server.

Refer

For more details on managing components, refer to Configuring and Monitoring Web Servers document.

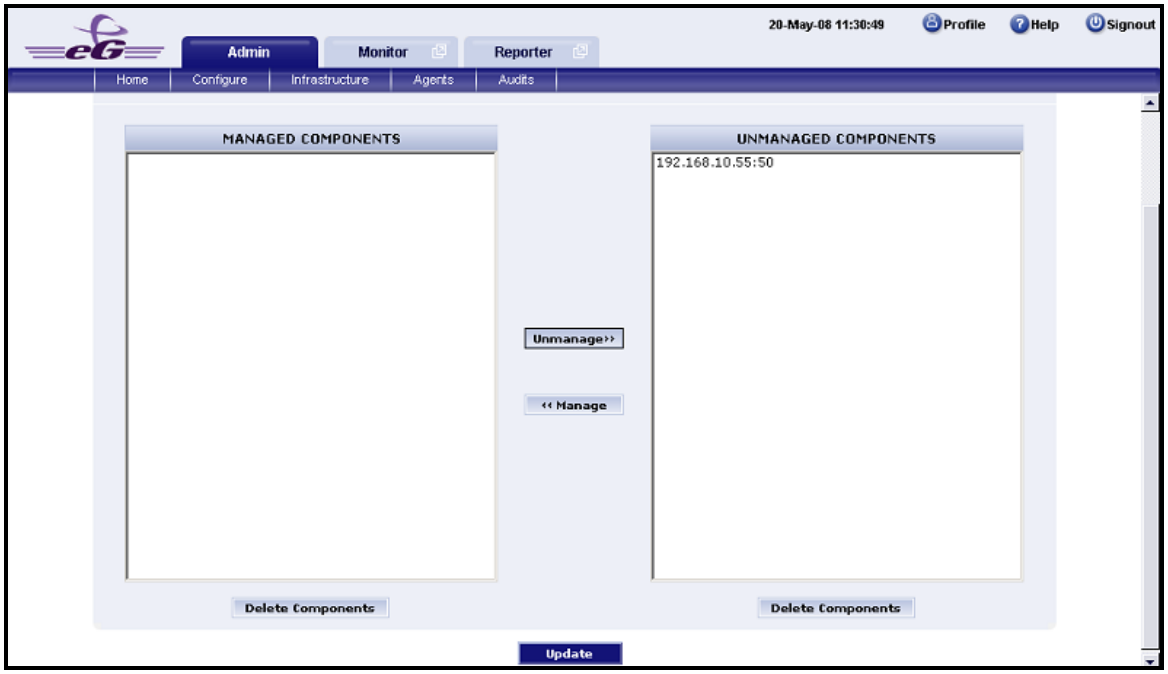

Figure 5.1: Selecting the Qmail server to be monitored

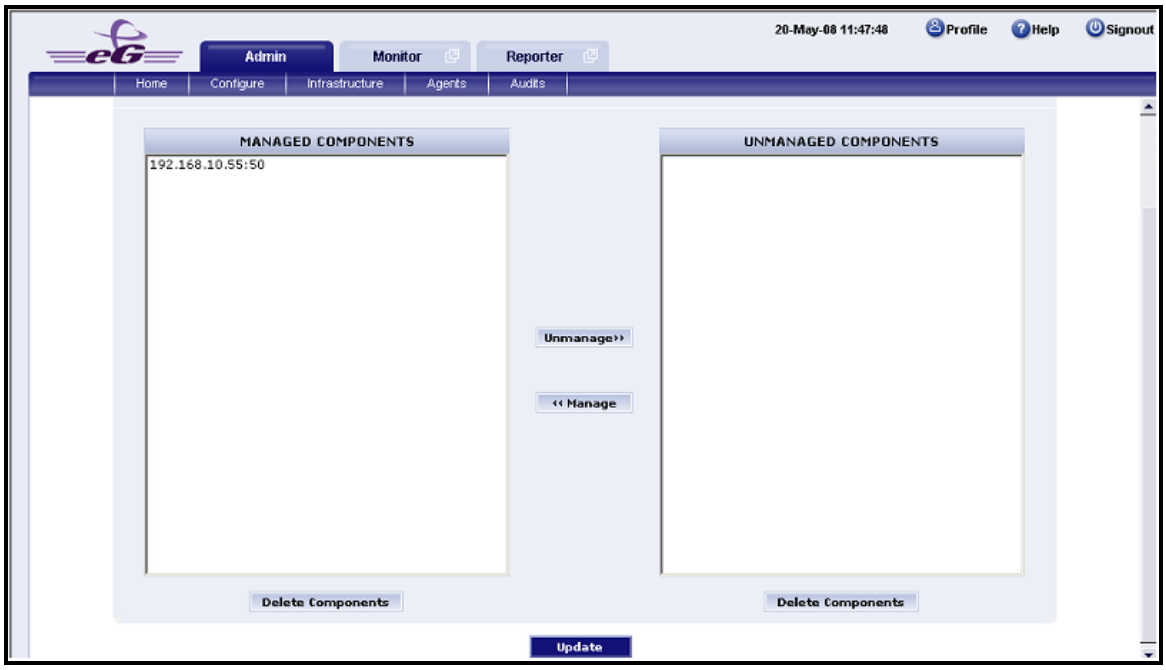

Figure 5.2: Managing the selected Qmail server

3. Now, try to sign out of the user interface. Doing so, will bring up the following page, which lists the unconfigured tests for the Qmail server.

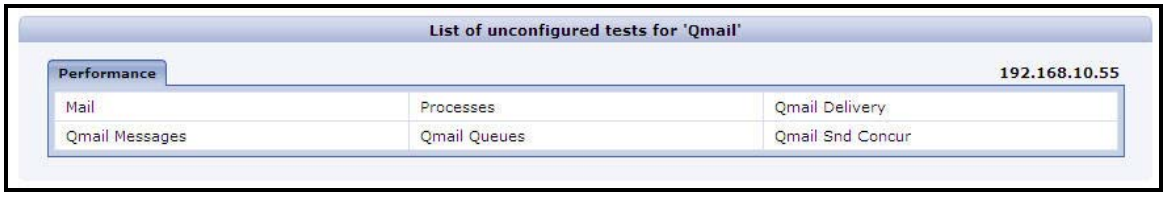

Figure 5.3: A page displaying the tests the need to be configured for the Qmail server

4. Click on the Qmail Delivery test to configure it. Figure 5.4 will then appear.

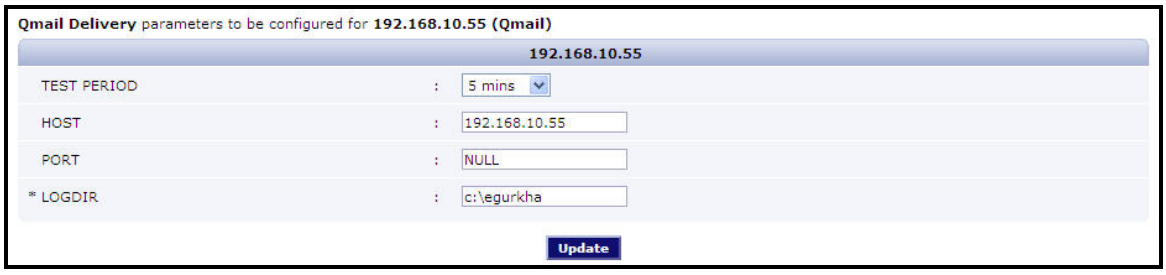

Figure 5.4: Configuring the Qmail Delivery test

5. Here, specify the following:
   - **TEST PERIOD** - How often should the test be executed
   - **HOST** –The host for which the test is to be configured

- **PORT** - The port at which the specified **HOST** listens
- **LOGDIR** – This test parses the qmail log files to extract the required measures. Therefore, in the LOGDIR text box here, specify the complete path to the qmail log directory, which stores the log files - for example, */var/log/qmail*.

6. Then, attempt to sign out of the administrative interface. When the **LIST OF UNCONFIGURED TESTS** appears, choose to configure the Qmail Queues test. Figure 5.5 will then appear.

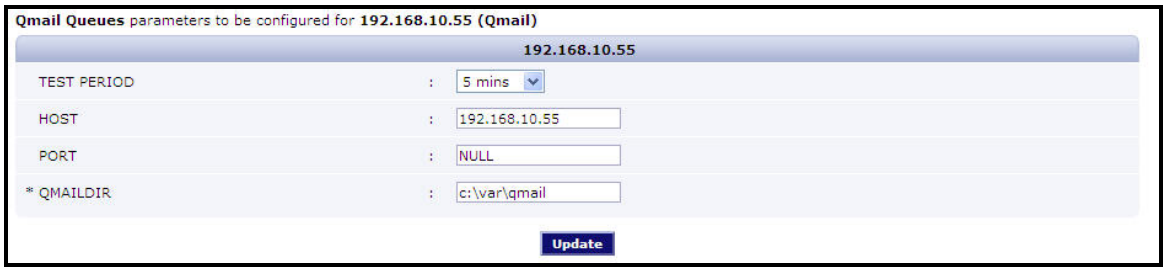

Figure 5.5: Configuring the Qmail Queues test

7. Here, specify the following:
   - **TEST PERIOD** - How often should the test be executed
   - **HOST** –The host for which the test is to be configured
   - **PORT** - The port at which the specified **HOST** listens
   - **QMAILDIR** – Specify the complete path to the Qmail install directory - for example, */var/qmail*.
8. Once again, try signing out of the administrative interface, and this time, click on Mail test in the **LIST OF UNCONFIGURED TESTS** to configure it.

Refer Please refer to Section 1.3 above for a more elaborate discussion on how to configure the Mail test.

9. After configuring the Mail test, try to sign out once again.
10. You will now be prompted to configure the Processes test.

Refer Please refer to Configuring and Monitoring Web Servers document for a more elaborate discussion on how to configure the Processes test.

11. Once the Processes test parameters are configured, log out of the administrative interface.

5.3 Monitoring the Qmail Server

1. Login as a monitor / supermonitor user.
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. Click on the *Qmail* server being monitored to view its measurements.

Chapter 6

Configuring and Monitoring the Instant Messenger of the Exchange 2000 Server

This chapter outlines the steps involved in configuring and monitoring the Instant Messenger of the Exchange 2000 Server.

6.1 Administering the eG Manager to Work with the Instant Messenger

To achieve this, do the following:

1. Login to the administrative interface of eG as an administrator (admin).
2. Manually add a component of type *Exchange Messaging* using the **ADD/MODIFY COMPONENTS** page (see Figure 6.1). To navigate to the **ADD/MODIFY COMPONENTS** page, follow the menu sequence: Infrastructure-> Components -> Add/Modify.

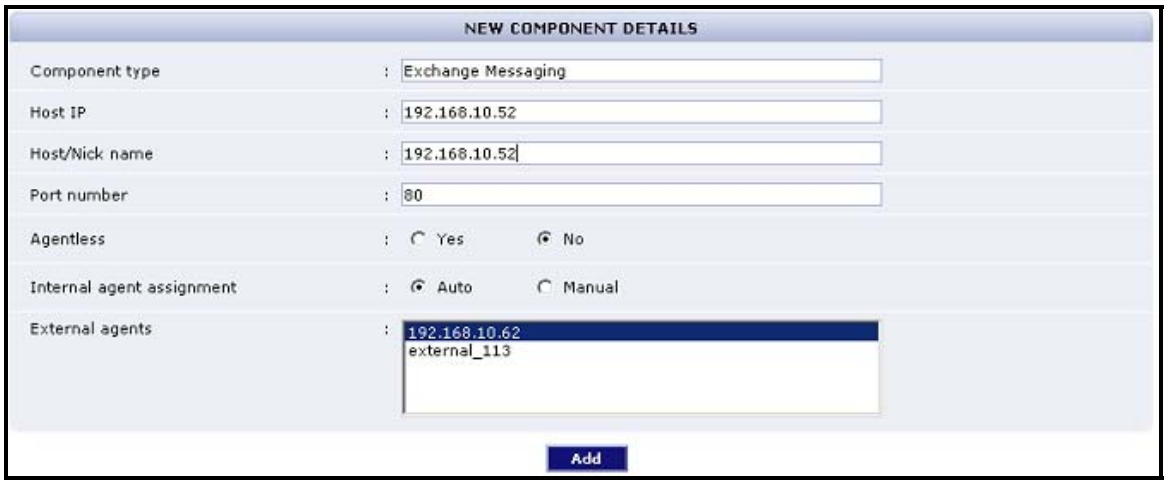

Figure 6.1: Adding the Instant Messenger

3. In Figure 6.1 that appears, specify the **Host IP** address of the Messenger, the **Host/Nick name**, and the **Port number** of the Instant Messenger. Then, click the **Add** button to register the changes. The Messenger server so added will be managed automaticalely by eG Enteprise.

4. Finally, sign out of the administrative interface.

6.2 Monitoring the Instant Messenger

1. Login as a monitor / supermonitor user.
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. Click on the Instant Messenger server being monitored to view its measurements:

Chapter 7

Configuring and Monitoring External Mail Servers

The generic *Mail* model offered by eG Enterprise requires that an agent be deployed on the mail server being monitored, so that the critical processes running on the mail server host, their resource utilization, and other OS-level metrics are extracted from within the host. However, sometimes, host-level metrics might not interest administrators as much as the availability of the server and its ability to send or receive mails. Therefore, to enable administrators to extract only external metrics such as availability and responsiveness, the eG Enterprise suite prescribes the *External Mail* server model. To use this model, an external agent would suffice. This agent employs native application-level protocols to determine the overall network health, mail server availability, and how quickly the server processes mails.

7.1 Administering the eG Manager to Work with an External Mail Server

To administer eG so that it monitors the External mail server, do the following:

1. Login as an administrator to the eG administrative interface.
2. Next, add the external mail server manually using the **ADD/MODIFY COMPONENTS** page (Infrastructure -> Components -> Add/Modify) (see Figure 7.1). Components manually added will be automatically managed by the eG Enterprise system (see Figure 7.1).

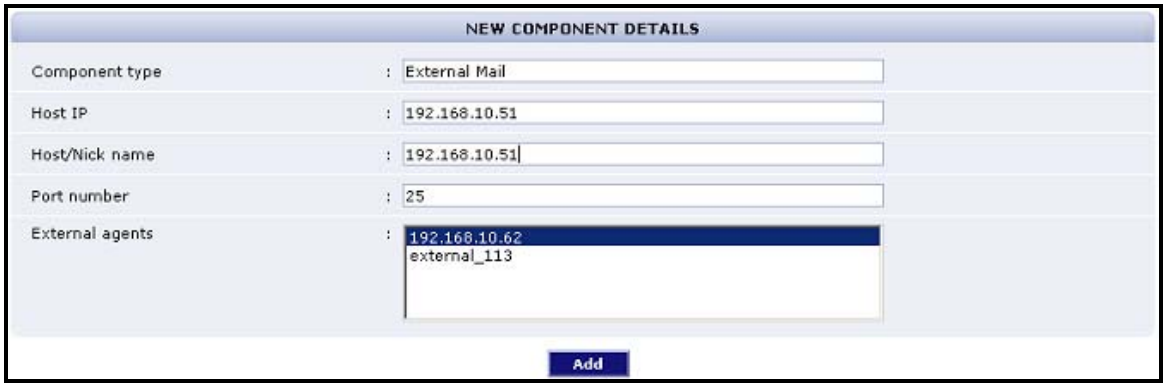

Figure 7.1: Adding an External mail server

3. Now, when you try to sign out, the following screen will appear, prompting you to configure the Mail test.

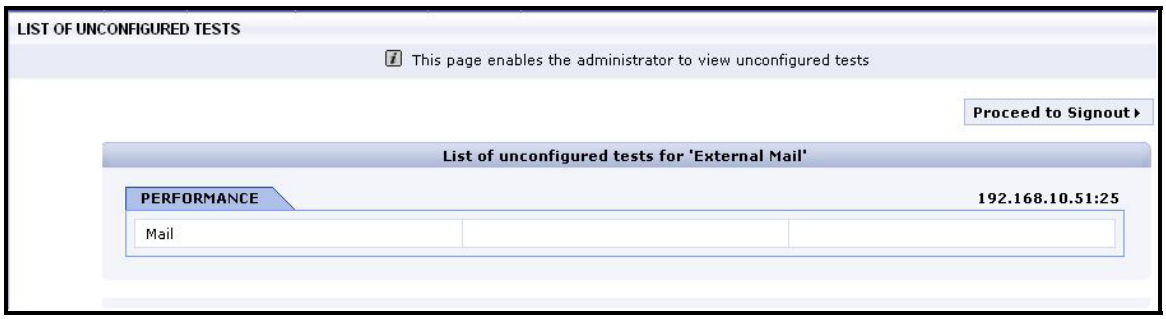

Figure 7.2: A page listing the unconfigured tests for the External mail server

4. Click on the **Mail test** entry in this page to configure it.

Refer Please refer to Section 1.3 above for a more elaborate discussion on how to configure the Mail test.

5. Then, click the **Update** button in the Mail test configuration page to update the configuration.
6. Finally, sign out of the administrative interface.

7.2 Monitoring the External Mail Server

1. Login as a monitor / supermonitor to the eG monitor user interface
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. Click on the independent *External Mail* server to view its measurements.

Chapter 8

Configuring and Monitoring the External Exchange Server

eG Enterprise prescribes an *Exchange* server model (already discussed) that requires an agent to be deployed on the Exchange 2000/2003/2007 server to continuously monitor its internal health. However, some administrators might only want to determine whether the mail server is available or not, and if so, how responsive it is to client requests. To capture and view such external metrics alone, eG Enterprise offers the exclusive, *External Exchange* model. Using a single eG external agent and no application-level instrumentation, the *External Exchange* model can indicate the availability of the Exchange mail server, the efficiency with which it processes messages, the overall health of the network connection between the agent host and the mail server host, and the availability of critical TCP ports on the mail server.

8.1 Administering the eG Manager to Work with an External Exchange Server

To administer eG so that it monitors the External Exchange server, do the following:

1. Login as an administrator to the eG administrative interface.
2. Next, add the external Exchange server manually using the **ADD/MODIFY COMPONENTS** page (Infrastructure -> Components -> Add/Modify) (see Figure 8.1). Components manually added will be automatically managed by the eG Enterprise system (see Figure 8.1).

Figure 8.1: Adding an External Exchange server

3. Now, when you try to sign out, the following screen will appear, prompting you to

configure the Mail test.

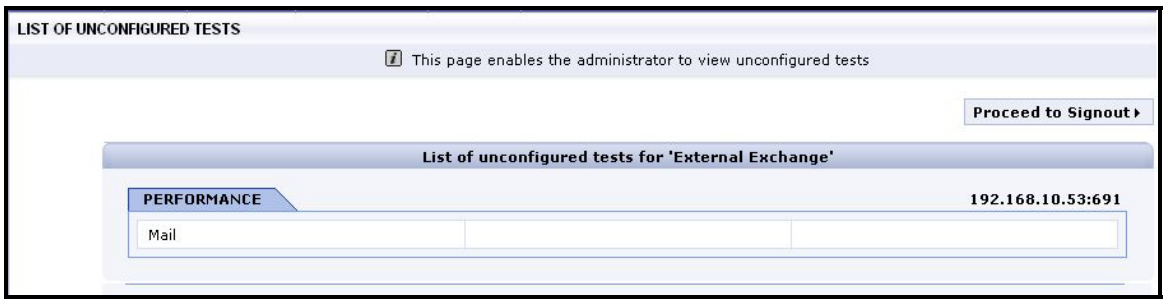

Figure 8.2: A page listing the unconfigured tests for the External mail server

4. Click on the **Mail** test entry in this page to configure it.

Refer Please refer to Section 1.3 above for a more elaborate discussion on how to configure the Mail test.

While configuring the Mail test, ensure that the port numbers (**SENDPORT** and **RECEIVEPORT**), user names (**SENDUSER** and **RECEIVEUSER**), the email IDs (**FROMID** and **TOID**), and the **RECEIVEHOST** configured for the test are applicable to all the Exchange servers that are in the cluster.

5. Then, click the **Update** button in the Mailtest configuration page to update the configuration.
6. Finally, sign out of the administrative interface.

8.2 Monitoring the External Mail Server

1. Login as a monitor / supermonitor to the eG monitor user interface
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. Click on the independent *External Mail* server to view its measurements.

Chapter 9

Configuring and Monitoring the Exchange Cluster Service

An Exchange cluster service is a collection of physical Exchange mail servers that can act as a single logical server. Requests to a cluster are routed through a virtual cluster server that is assigned a cluster IP address and TCP port. Requests to this server can be handled by any of the individual nodes in the cluster at any given point in time, depending on which node is active at that time.

Since clusters are deployed in environments where 24*7 availability and responsiveness are critical, it is imperative that the performance of the clusters is monitored all the time.

9.1 Administering the eG Manager to Work with an Exchange Cluster Service

To monitor an Exchange cluster, an eG external agent is deployed, which emulates a mail send-receive activity on the Exchange cluster. The emulated requests are directed at the virtual cluster server. Therefore, you need to manage the virtual cluster server as an *Exchange Cluster* using the eG administrative interface. To achieve this, do the following:

1. Login as an administrator to the eG administrative interface
2. Next, add the virtual cluster server as the Exchange cluster using the **ADD/MODIFY COMPONENTS** page (Infrastructure -> Components -> Add/Modify) (see Figure 9.1). Components manually added will be automatically managed by the eG Enterprise system (see Figure 9.1).

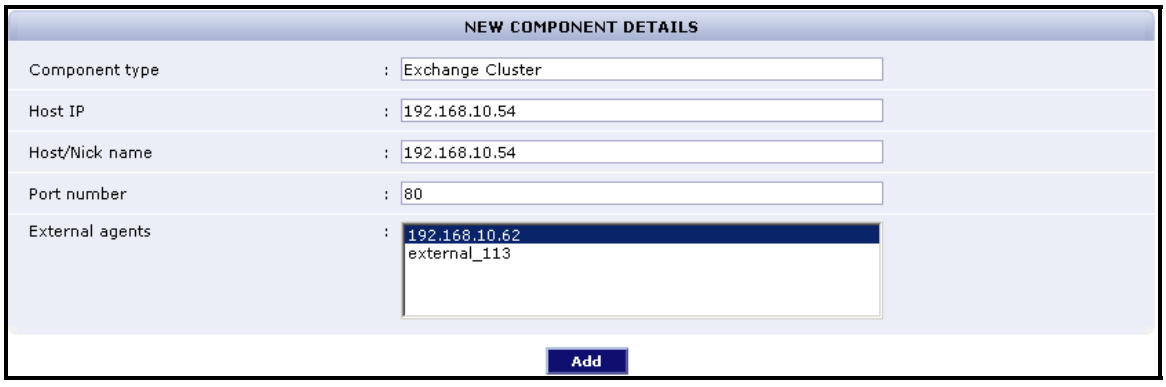

Figure 9.1: Adding an Exchange cluster service

3. Next, manage/manually add the individual Exchange servers that form part of the cluster.

Refer Please refer to section 3.2 above for a more elaborate discussion on how to manage an Exchange server using the **MANAGE/UNMANAGE** page.

4. Then, configure a new segment, where the *Exchange Cluster* shares a **USES** relationship with all the individual Exchange servers in the cluster. The cluster service is deemed healthy if the user requests are served by at least one of the servers in the cluster.

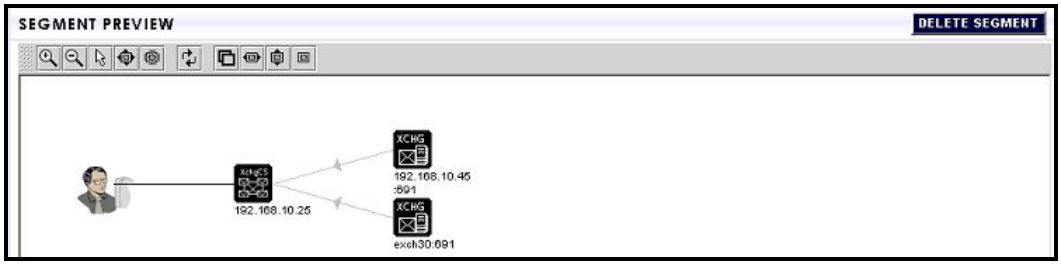

Figure 9.2: A segment containing the cluster service and the Exchange servers

5. Ensure that an external agent monitors the *Exchange Cluster*, and internal agents are deployed on the individual Exchange servers in the cluster to monitor their internal operations.
6. Now, when you try to sign out, the following screen will appear.

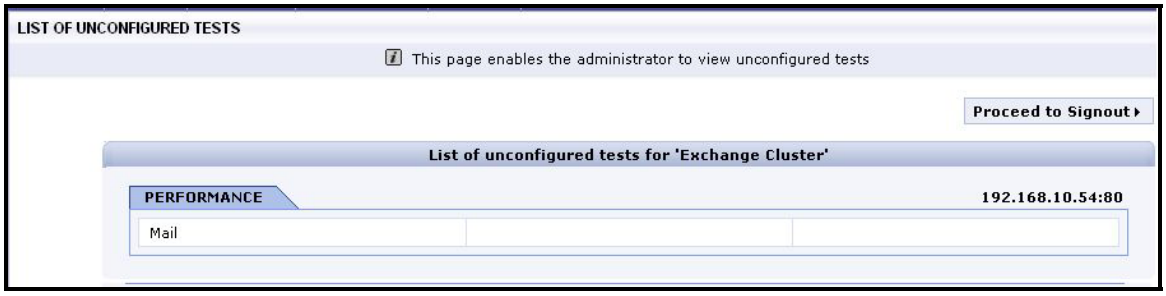

Figure 9.3: A page listing the unconfigured tests for the Extchange cluster service and the individual Exchange servers in the cluster

7. Configure the Mail test and DisconnectedMailBox test for each of the Exchange servers in the cluster, in the manner already discussed.

Note:

While configuring the Mail test for a passive Exchange server in the cluster, set the **IS PASSIVE** flag to **YES**. Doing so ensures that no alerts are generated if the server is not running. Measures will be reported as "Not applicable' by the agent if the server is not up. However, the internal agent executing on the stand-by server will continue to alert the administrator of operational issues with the server such as too many open sessions to the server, unusual lock behavior, etc.

While configuring the Mail test for an active Exchange server in the cluster, set the **ISPASSIVE** flag to **NO**. This ensures that as soon as the server becomes unavailable, eG Enterprise sends out an alert.

8. Then, click on the **Mail test** of the *Exchange Cluster* to configure it.

Please refer to section 1.3 above for a more elaborate discussion on how to configure the Mail test.

While configuring the Mail test, ensure that the port numbers (**SENDPORT** and **RECEIVEPORT**), user names (**SENDUSER** and **RECEIVEUSER**), the email IDs (**FROMID** and **TOID**), and the **RECEIVEHOST** configured for the test are applicable to all the Exchange servers that are in the cluster.

9. Then, click the **Update** button in the **TEST CONFIGURATION PAGE** to update the configuration.
10. Finally, sign out of the administrative interface.

9.2 Monitoring the Exchange Cluster Service

1. Login as a monitor / supermonitor to the eG monitor user interface.
2. Click on the **Segments** option in the menu, select the segment representing the Exchange cluster, and click on the Exchange cluster service component to view its measurements.

For an in-depth discussion on eG Enterprise's Cluster Monitoring capabilities and to understand the implications of cluster availability on service performance, refer to the *Monitoring Clusters Using eG Enterprise* chapter (Chapter 7) in the *eG User Manual*.

Chapter 10

Configuring and Monitoring the IronPort AsyncOS Mail Server

The IronPort AsyncOS Mail Server can be configured and monitored by following the steps given below:

- Administer the eG manager to monitor the IronPort AsyncOS Mail Server
- Monitor the IronPort AsyncOS Mail Server

10.1 Administering the eG Manager to monitor an IronPort AsyncOS Mail Server

1. Login to the administrative interface of eG as an administrator (admin).
2. Manually add the *IronPort AsyncOS Mail* Server to be monitored using the **ADD/MODIFY COMPONENTS** page (see Figure 10.1). To navigate to the **ADD/MODIFY COMPONENTS** page, follow the menu sequence: Infrastructure -> Components -> Add Modify.
3. To add a new asyncos mail server, first, select **IronPort AsyncOS Mail** as the **Component type** (as shown Figure 10.1 below) and then, click the **Add New Component** button.

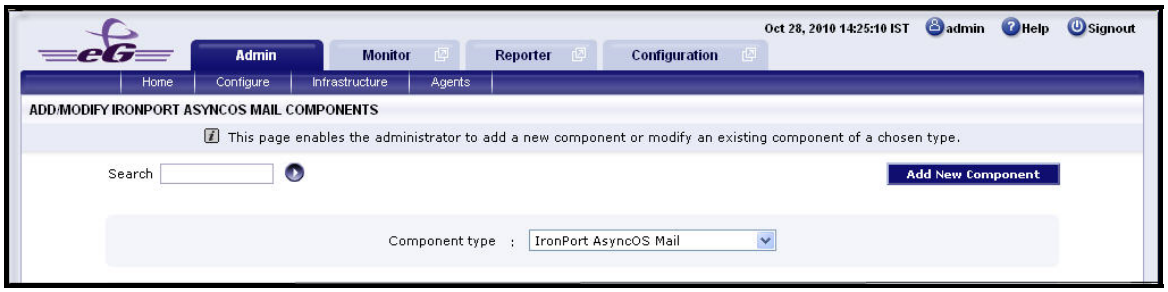

Figure 10.1: Selecting the type of component to be added

4. The following page (Figure 10.2) will then appear. Specify the Host IP address of the new mail server, and the Nick name of the mail server. Then, click the **Add** button to register the changes.

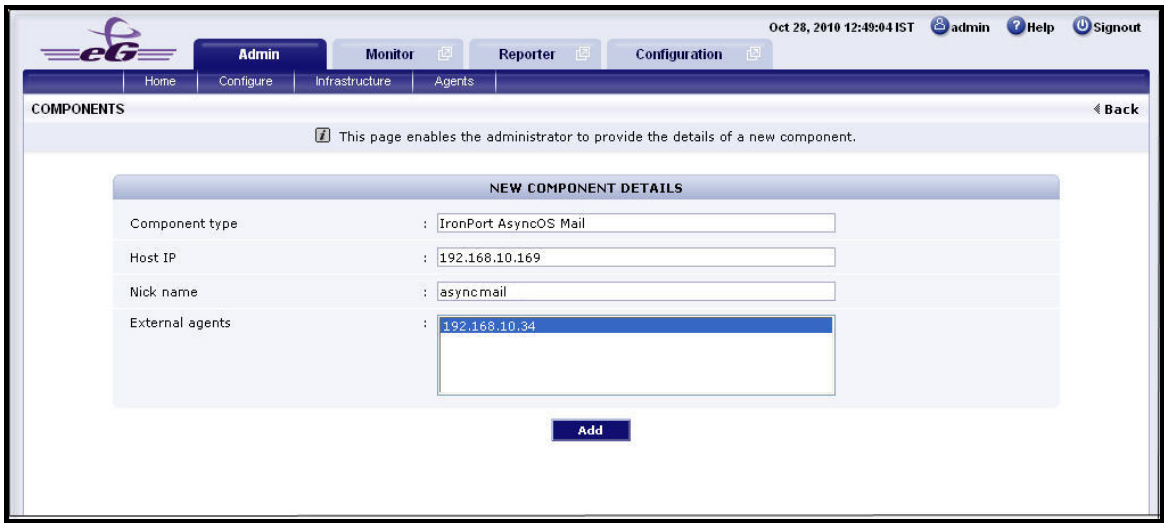

Figure 10.2: Adding the details of a new IronPort AsyncOS Mail Server

5. A summary of the new component details will then appear as shown in Figure 10.3 below.

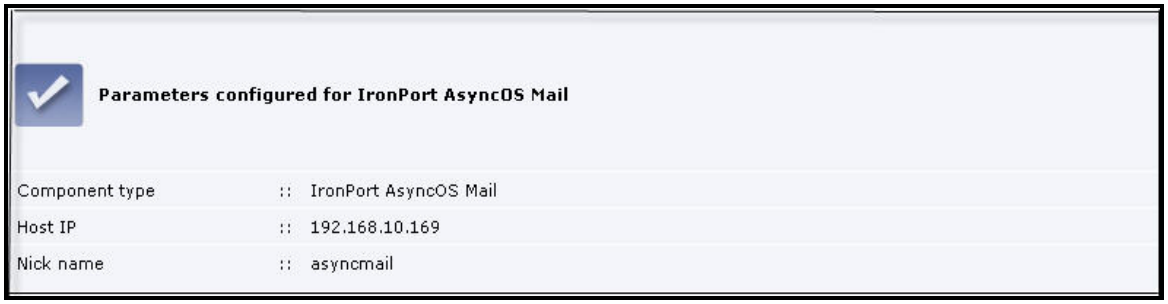
Parameters configured for IronPort AsyncOS Mail
Component type :: IronPort AsyncOS Mail
Host IP :: 192.168.10.169
Nick name :: asyncmail

Figure 10.3: A page displaying a summary of the new IronPort AsyncOS Mail Server details

6. The IronPort AsyncOS Mail Server so added will be managed automatically by eG Enterprise. Now, try to sign out of the user interface. Doing so, will bring up the following page, which prompts you to configure a list of unconfigured tests (see Figure 10.4) for the new IronPort AsyncOS Mail Server.

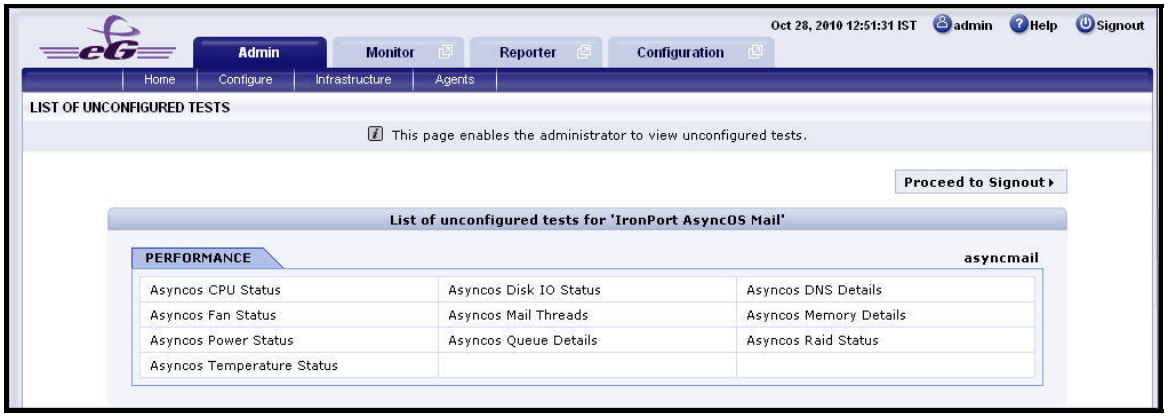

Figure 10.4: A page displaying the tests that need to be configured for the IronPort AsyncOS Mail Server

7. Click on Asyncos Fan Status test to configure it. Figure 10.5 will then appear.

Asyncos Fan Status parameters to be configured for asyncmail (IronPort AsyncOS Mail)
ASYNCMAIL
TEST PERIOD : 5 mins
HOST : 192.168.10.169
SNMPPORT : 161
TIMEOUT : 10
SNMPVERSION : v1
* SNMPCOMMUNITY : public
APPLY TO OTHER COMPONENTS :
Update

Figure 10.5:Configuring the Asyncos Fan Status test

8. Here, specify the following:

- **TEST PERIOD** – How often should the test be executed
- **HOST** - The host for which the test is to be configured.
- **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161.
- **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
- **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
- **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
- **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
- **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
- **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
- **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

- **MD5** – Message Digest Algorithm
- **SHA** – Secure Hash Algorithm

- **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
- **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
  - **DES** – Data Encryption Standard
  - **AES** – Advanced Encryption Standard
- **ENCRYPTPASSWORD** – Specify the encryption password here.
- **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

9. Click the **Update** button to configure the test.
10. Finally, signout of the administrative interface.

10.2 Monitoring the IronPort AsyncOS Mail Server

1. Login as a monitor / supermonitor user.
2. Click on the **Components** option in the menu bar, and select the **Servers** option from the **Components** menu.
3. Click on the *IronPort AsyncOS Mail* Server being monitored to view its measurements.

Chapter 11

Troubleshooting

If Mail test does not work, then check whether the user account being configured for Mail test to retrieve mails from POP3 is valid. To do so, do the following:

```
<Command to enter>telnet <serverIP> 110
<server response:> +OK DPOP Version number supressed.
<Command to enter>USER john
<server response:> +OK john nice to hear from you - password required
<Command to enter>PASS <Your password>
<server response:> +OK john has 0 mail messages
<Command to enter>LIST
<server response:> +OK 0 (0)
<Command to enter>quit
<server response:> +OK bye john
```

To check whether you are able to send mails, do the following:

```
<Command to enter> telnet <SMTP Server IP> 25
<server response:> 220 eginnovations.com DSMTP ESMTP Mail Server
<Command to enter> HELO localhost
<server response:> 250 eginnovations.com. Hello localhost (61.11.72.169)
<Command to enter> MAIL FROM: mailto:victor@eginnovations.com
<server response:> 250 Command MAIL OK
<Command to enter>RCPT TO: mailto:john@eginnovations.com
<server response:> 250 Command RCPT OK
<Command to enter>DATA
<server response:> 354 Command DATA Start mail input; end with
<CRLF>.<CRLF>
<Command to enter>Subject: This is a test message
```

```
This message is a test message to check the eG mail test.
..                    <End                    with                    ".">
<server response:> 250 Command DATA Processed mail data Ok
<Command                          to                          enter>quit
<server response:> 221 Command QUIT eginnovations.com Service closing
transmission channel to local host
```

While checking, ensure that you provide the same values that were provided while configuring MailTest. There could be instances where "john" would be allowed access to Pop3 mails but "john@eginnovations.com" may not have rights to check mails.

Chapter 12

Conclusion

This document has described in detail the steps for configuring and monitoring the **Mail servers**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.